N° 3560

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 22 juin 2011.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA MISSION D'INFORMATION COMMUNE

sur **les droits** *de l'***individu** *dans la* **révolution numérique** [1]

ET PRÉSENTÉ

PAR MM. PATRICK BLOCHE ET PATRICE VERCHÈRE

Députés.

(1) La composition de cette mission figure au verso de la présente page.

La mission d'information commune à la Commission des affaires culturelles et de l'éducation et à la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les droits de l'individu dans la révolution numérique est composée de : M. Jean-Luc Warsmann, président ; M. Sébastien Huyghe, Mme Marietta Karamanli, vice-présidents ; M. Patrick Bloche et M. Patrice Verchère, rapporteurs ; Mme Brigitte Barèges, M. Serge Blisko, M. Bruno Bourg-Broc, M. Jean-Pierre Brard, M. Olivier Dussopt, M. Jean-Jacques Gaultier, Mme Françoise Guégot, M. Jean-Christophe Lagarde, Mme Muriel Marland-Militello, Mme Martine Martinel, Mme Françoise de Panafieu, M. Christian Paul, M. Franck Riester, M. Marcel Rogemont, M. Jean-Sébastien Vialatte.

SOMMAIRE

Pages

MESDAMES, MESSIEURS,

Le Parlement et la révolution numérique : tout semblerait en apparence les opposer.

D'un côté une institution multiséculaire, fondée sur la collégialité, nationale, aux procédures rigoureuses et souvent longues ; de l'autre, un foisonnement de novations dans une juvénilité sans cesse renouvelée, l'individualité sublimée, l'absence de frontières, le refus du formalisme, l'immédiateté.

Et pourtant comment le Parlement – qui, notons-le, a d'ailleurs parfaitement su se mettre à l'heure du numérique [(1)] – pourrait-il ignorer cette révolution qui non seulement remodèle, dans un processus d'inventions perpétuelles, les rapports politiques, économiques et sociaux, mais affecte aussi les individus dans ce qui les constitue profondément ?

Au printemps 2010, la commission des Lois et la commission des Affaires culturelles de l'Assemblée nationale ont souhaité relever le défi en s'attaquant à une question – on devrait écrire plutôt une myriade de questions – qui, plus que toute autre, justifie que les députés s'y intéressent : **quelles sont les conséquences de la révolution numérique sur les droits de l'individu ?**

Ce thème s'est naturellement imposé en raison des bouleversements que connaissent aujourd'hui les conditions dans lesquelles s'exercent les droits individuels dans l'univers numérique et des grands débats qui émergent dans nos sociétés. Quelles sont, sur le Net, les données personnelles qui circulent aujourd'hui sur chacun d'entre nous ? Qui en a la maîtrise et peut les exploiter ? À

(1) Les vidéos des auditions sont consultables sur le site de l'Assemblée nationale : www.assemblee-nationale.fr.

quelles fins ? Existe-t-il un droit à l'oubli qui permettrait de faire disparaître les informations nous concernant et qui figurent sur *Google* ou *Facebook* ? Peut-on échapper au pistage électronique, à la géolocalisation, aux puces *RFID* qui, minuscules et invisibles, pourraient dévoiler les moindres recoins de notre vie quotidienne ? La publicité comportementale est-elle une menace ? Et finalement peut-on faire le choix de ne pas exister numériquement ?

Mais cet univers numérique n'est pas seulement riche de questions plus ou moins inquiétantes ; il est également un nouveau continent qui s'offre à chacun d'entre nous avec des potentialités insoupçonnées. L'accès à la culture, la rencontre avec l'autre, la capacité à s'exprimer plus directement dans un cadre démocratique renouvelé, la faculté de mieux communiquer avec les administrations pour mieux se faire comprendre et respecter par l'État, telles sont aussi les opportunités qui s'ouvrent devant chaque citoyen pour peu qu'il sache comment maîtriser correctement ces nouvelles techniques, s'orienter dans ce dédale virtuel et agir en connaissance de cause.

On le voit, l'enjeu est de taille et **le Parlement a une double vocation à intervenir**. Comme institution démocratique, il lui appartient de tracer des perspectives communes à tous les citoyens, là où le monde numérique s'adresse à des individus ou des groupes isolés constituant autant de fragments dans notre société. Comme législateur, le Parlement a évidemment vocation à protéger, par la loi, les droits fondamentaux, à les concilier lorsqu'ils entrent en contradiction, à les encadrer quand l'usage qu'en font certains menace la liberté d'autres citoyens.

« Les droits de l'individu dans la révolution numérique » : les termes méritent d'être précisés. La mission d'information a souhaité ne pas se restreindre dans le champ de ses investigations. Elle assume ce choix consistant à offrir la vision la plus large possible des questions qui se posent désormais à chacun d'entre nous dans l'exercice de ses libertés au sein de l'univers numérique.

Par droits de l'individu, la mission a entendu évoquer les libertés et les droits fondamentaux dans l'acception la plus large, que ce soit les libertés individuelles comme la vie privée, les libertés politiques comme le droit d'expression, de vote, ou les droits sociaux comme le droit à l'éducation [(1)].

Sous les termes « révolution numérique », il faut, là encore, voir la volonté d'embrasser le plus largement possible les nouvelles techniques qui se déploient, chaque jour, sous nos yeux. Par numérique, il faut entendre l'ensemble des nouvelles technologies de l'information et de la communication (TIC), qui, utilisant des signaux numériques[(2)], notamment dans la reproduction et la diffusion

---

(1) On observera que la mission n'a pas souhaité revenir sur la question des droits d'auteur des fichiers de police et de la cybercriminalité qui ont fait l'objet de débats très approfondis lors de l'examen de récents projets de loi.

(2) Le dictionnaire Robert *en donne la définition suivante : «* adj. *Se dit de la représentation de données ou de grandeurs physiques sous forme de nombres (par oppos. à* analogique*) et par ext. de systèmes, dispositifs ou procédés employant ce mode de représentation. […]* N. m. *Le numérique : l'ensemble des techniques de communication qui utilisent des signaux numériques, notamment dans la reproduction des images*. »

des images, permettent de générer, de traiter, de mettre en réseau, d'échanger et d'archiver d'importants flux de données. Nous avons considéré, pour parler plus concrètement, principalement Internet et les services qu'il offre, mais aussi des dispositifs nouveaux comme les puces *RFID,* qualifiées parfois d'« Internet des objets ». Cependant la mission n'a pas entendu aborder plus précisément la question des nanotechnologies qui constitue un sujet en soi et qui, par ailleurs, a déjà fait l'objet de travaux parlementaires, comme ceux de l'office parlementaire d'évaluation des choix scientifiques et technologiques (1).

La révolution numérique, expression aujourd'hui courante, peut, quant à elle, être définie comme cette conjonction historique de la numérisation généralisée de l'information et de sa mise en réseau au niveau planétaire, *via* Internet (2), qui constitue non pas une simple rupture technologique mais bien une révolution en raison de ses conséquences sur nos comportements, nos manières de pensées et sur l'organisation politique, économique, sociale et culturelle de nos sociétés dans un monde global.

La mission d'information a souhaité, dès l'origine, mener un travail approfondi, sur une année. Elle a ainsi procédé à 45 auditions, entendu plus de cent personnes représentant tous les acteurs concernés comme en atteste la liste des personnes reçues par la mission figurant en annexe de ce rapport. Les rapporteurs se sont rendus aux États-Unis en février 2011 et, on le verra, des relations très étroites se sont nouées avec les députés allemands du *Bundestag* qui ont constitué au printemps 2010 une commission d'enquête sur le même thème.

Faisant le choix d'un travail à long terme, la mission a assumé un risque : celui de devoir sans cesse renouveler ses informations tant les techniques numériques et les enjeux qui s'y attachent évoluent rapidement. Chaque jour, un événement nouveau intervient qui change la donne, apporte des éclairages inédits au risque de laisser penser que ce qui a été écrit sera déjà dépassé au moment même où il sera publié. Les membres de la mission ont conscience de cette situation de fait mais ne la surestiment pas non plus car l'ambition de ce rapport n'est pas de faire un état des avancées technologiques. Il s'agit de tracer des perspectives, d'offrir des repères à nos concitoyens dans un monde virtuel qui en manque parfois cruellement en substituant trop souvent à l'ordre des valeurs communes celui des seuls désirs particuliers.

Sur le fond, une ligne de conduite a guidé la mission ; elle figure à l'article premier de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie*

(1) Office parlementaire d'évaluation des choix scientifiques et technologiques, Les nanotechnologies. Risques potentiels, enjeux éthiques, *n*os *3658 et 208, février 2007.*

(2) Voir Laurent Sorbier, « Quand la révolution numérique n'est plus virtuelle… », Esprit, *n° 324, mai 2006, p. 121.*

privée, ni aux libertés individuelles ou publiques. » Si on substitue ici le terme « numérique » à « informatique », on voit apparaître les deux axes de ce rapport.

La mission a, dès l'origine, rejeté l'idée que le monde numérique ne serait lourd que de menaces. À aucun moment, les membres de la mission n'ont souhaité laisser libre cours à cette forme de scepticisme, qui fait parfois figure de prêt-à-penser, selon lequel les progrès considérables que nous offre la révolution numérique conduiraient à la destruction subreptice de nos libertés. Au contraire, la mission a entendu mettre en évidence les perspectives nouvelles et tangibles qui peuvent trouver à s'exprimer en termes de droit d'expression, d'accès à l'éducation, à la culture, de participation politique…

Mais l'enthousiasme que peut susciter la révolution numérique – dont chacun d'entre nous profite au quotidien – ne doit pas confiner à une forme de naïveté. Les individus ne peuvent rester démunis face à la puissance des grandes entreprises du numérique. Ils doivent aussi pouvoir trouver auprès des autorités publiques des relais pour se faire entendre, pour que leurs droits fondamentaux soient respectés.

La mission a donc entendu montrer que la révolution numérique était un formidable instrument de *promotion* des droits mais qu'il fallait aussi assurer une *protection* de ces droits dans ce nouvel univers. À cette fin, le présent rapport est articulé autour de quatre grands moments.

Le premier consiste à montrer en quoi **Internet est au service des droits de l'individu** en ce qu'il constitue un vecteur sans précédent de la liberté d'expression et de communication mais aussi d'accès à l'information, à la connaissance et à la culture. À partir de là, de nouveaux droits ou de nouvelles modalités d'exercice de ces droits émergent comme la *e*-démocratie ou l'accès aux services administratifs par voie numérique.

Le deuxième temps portera sur **le droit à une protection de l'individu dans l'univers numérique**. Il y sera question du respect de la vie privée, de la possibilité, ou non, d'un droit à l'oubli et plus largement de la protection des données personnelles que ce soit face au « *cloud computing* » ou « informatique dans les nuages », aux failles de sécurité, au ciblage publicitaire… L'accent sera porté notamment sur la protection des mineurs qui sont les plus ouverts à cet univers numérique mais aussi les plus exposés à certains de ses débordements.

Le troisième moment sera consacré au **droit à l'accès à Internet**. À travers la question de la neutralité du Net et de la fracture numérique, il s'agit de préserver la possibilité pour chacun, qu'il consulte Internet ou s'y exprime, d'accéder à cet instrument aujourd'hui essentiel à l'exercice de ses libertés.

Enfin, en conclusion, sera posée la question de la **gouvernance et de la régulation de l'univers numérique.** On constate que les leviers classiques que sont l'action de l'État, en particulier par la loi, demeurent essentiels mais qu'il convient également d'utiliser d'autres instruments plus souples qui engagent les

grands acteurs du monde numérique sous l'œil des citoyens. À l'évidence, pour peser face aux grands groupes mondiaux, les États européens doivent fédérer leurs points de vue, l'Union européenne ayant un rôle éminent à jouer en la matière. Dans cette optique, les initiatives franco-allemandes, comme celle que la mission a prise avec son homologue du *Bundestag,* prennent tout leur sens.

*
* *

La mission d'information a souhaité non pas, comme à l'accoutumée, faire une liste de propositions ; elle a entendu plutôt fixer **54 orientations pour l'avenir.** Certaines se déclinent en propositions précises ; d'autres déterminent un cap.

En effet, il a paru à la mission d'information que, pour promouvoir les droits de l'individu dans et par le numérique, l'essentiel était d'offrir à chaque **« citoyen numérique »** la possibilité de choisir en connaissance de cause. Face à la révolution numérique, la déploration ou l'exaltation doivent se voir substituer la lucidité du citoyen éclairé, dès son plus jeune âge, qui pourra faire le choix de paraître ou non sur le Net en dévoilant une part plus ou moins grande de sa vie personnelle, en ayant la capacité de refuser, de changer d'avis, de peser non seulement face aux grands groupes mais aussi à une forme de pression ou de contrôle social numérique.

On l'aura compris, l'ambition de ce rapport est à la fois modeste – la mission ne prétend pas répondre définitivement à la multitude de questions qui s'offre à nous – et très grande – en ce qu'elle entend tracer des perspectives permettant de structurer les débats de demain. Ce rapport est aussi à l'image de cette révolution numérique qui connecte le particulier à l'universel et fait de chacun l'acteur d'une scène désormais mondiale. C'est en s'adressant au « citoyen numérique », en lui permettant d'user de sa raison et de sa liberté, que l'on pourra **faire de l'univers numérique un lieu d'épanouissement des droits des individus.**

TITRE PREMIER

L'INTERNET AU SERVICE

DES DROITS DE L'INDIVIDU

PREMIÈRE PARTIE : LA LIBERTÉ D'EXPRESSION ET DE COMMUNICATION, L'ACCÈS À L'INFORMATION, LA CONNAISSANCE ET LA CULTURE À L'ÈRE NUMÉRIQUE

Si la « révolution numérique » n'est pas dépourvue de risques, l'impact positif des technologies numériques sur la vie des individus n'est plus à démontrer. Sources de progrès, de confort et de sécurité quotidiens, ils sont désormais si profondément intégrés dans nos modes de vie que leur disparition nous paraît aujourd'hui tout simplement inenvisageable.

La possibilité d'une transmission complète et instantanée d'informations dématérialisées nous permet, chaque jour, de communiquer avec nos proches et nos collègues, de profiter de biens et services culturels d'une diversité quasi infinie, de gérer à distance certaines formalités administratives, de prévoir au mieux nos itinéraires et temps de transport, de faire nos courses dans des magasins virtuels, de réserver des voyages, de comparer les prix des produits de grande consommation, de prendre part à des jeux virtuels en réseaux ...

Mais ce sont aussi nos droits, au premier rang desquels la liberté d'expression et de communication ainsi que l'accès à la culture et au savoir ainsi que la démocratie qui disposent, avec Internet, d'un instrument incroyable de promotion.

I. LA NOUVELLE DIMENSION DE LA LIBERTÉ D'EXPRESSION ET DE COMMUNICATION À L'ÈRE NUMÉRIQUE

A. INTERNET : UN OUTIL RÉVOLUTIONNAIRE

1. La consécration du rôle d'Internet par le Conseil constitutionnel

La liberté de communication et d'expression est consacrée par l'article 11 de la Déclaration des droits de l'homme et du citoyen, qui dispose que « *la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi* ».

Cette liberté, qui était, au moment de la Révolution française, celle de l'imprimeur et du journaliste, c'est-à-dire celle de « l'émetteur », est devenue, au fil du temps, celle du lecteur de journaux et de l'auditeur et du téléspectateur de radio et de télévision, c'est-à-dire celle du « receveur ».

Dans sa décision n° 2009-580 DC du 10 juin 2009, le Conseil a jugé « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et*

l'expression des idées et des opinions », l'exercice de la liberté de communication et d'expression impliquait la liberté d'accéder à Internet.

La protection constitutionnelle de la liberté de communication et d'expression s'applique à Internet compte tenu du rôle croissant que joue ce média dans l'accès du citoyen à l'information. Il s'agit de la dimension « passive » de la liberté d'expression qui a guidé le contrôle des lois relatives à la presse écrite et aux médias audiovisuels.

Mais le Conseil relève qu'Internet permet également, à travers la messagerie électronique, l'explosion des réseaux sociaux, des blogs et autres forums de discussion, d'exercer sa liberté d'expression dans sa dimension « active ». C'est en effet une caractéristique majeure de ce nouveau média que d'offrir à l'internaute la capacité de contribuer à la diffusion de l'information et de participer à la circulation et à l'échange d'idées et d'opinions.

M[e] Alain Bensoussan, avocat à la cour d'appel de Paris, au cours de son audition du 27 octobre 2010, a insisté sur le fait que tous les services proposés sur Internet n'étaient d'ailleurs pas réductibles à des médias. La liberté d'expression a été démultipliée grâce aux nouvelles technologies et à un modèle de financement par la publicité. Avant le développement de *Facebook*, seul un événement permettait de se faire connaître et la notoriété était réservée à quelques personnages de premier plan. Selon M[e] Alain Bensoussan, la réunion de 500 millions de personnes sur *Facebook* renvoie à un droit universel que l'on ne saurait réduire à un droit des médias mais qui constitue un droit de la vie, le droit de se présenter aux autres et de leur parler, *Twitter*, lui, correspondant à l'exercice du droit de « papoter ». Ainsi, la liberté prend-elle une dimension nouvelle, rendant possible par exemple la création d'événements de masse. Une telle liberté a toujours été désirée mais les médias traditionnels ne pouvaient lui donner toute sa portée.

Outre la censure du dispositif de sanction mis en place par loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet en tant qu'il habilitait la commission de protection des droits de la haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI) à couper l'accès à Internet de titulaires d'abonnement, pouvoir qui ne pouvait incomber qu'au juge, la reconnaissance du rôle d'Internet dans l'exercice de la liberté d'expression et de communication impose aux pouvoirs publics la mise en place de politiques favorisant la présence et la mise en valeur d'une information et de contenus de qualité sur Internet, l'éducation aux médias ainsi que l'accès à Internet dans des conditions satisfaisantes pour l'ensemble de nos concitoyens, ce qui passe à la fois par la protection de la neutralité de l'Internet et la lutte contre la fracture numérique. L'ensemble de ces thématiques sera abordé dans la suite du présent rapport.

2. La consécration du rôle d'Internet au plan international

Dans le cadre du Sommet mondial sur la société de l'Information en 2003 et 2005, l'ensemble de la communauté internationale – plus de 180 États – a reconnu la pleine applicabilité à l'Internet de la Déclaration universelle des droits de l'homme, en particulier de son article 19 relatif à la liberté d'expression et d'opinion. Internet a par ailleurs été qualifié de « *ressource publique mondiale* » par le sommet mondial sur la société de l'information (SMSI) et de « *bien public mondial* » par le Parlement européen.

Comme l'a rappelé M. Bernard Kouchner, ministre des Affaires étrangères et européennes, dans son discours d'ouverture d'une réunion consacrée à Internet et la liberté d'expression qui rassemblait une soixantaine de participants, représentants de dix-sept gouvernements, d'organisations non gouvernementales, d'entreprises et d'organisations internationales et qui s'est tenue le 8 juillet 2010 au ministère des Affaires étrangères et européennes, « *avec le développement d'Internet, jamais la liberté d'expression et de communication n'aura connu telle révolution ! S'appuyant sur des techniques toujours plus puissantes, les mots, les images, les savoirs circulent à une vitesse accélérée dans un espace sans frontières. Un espace sans équivalent pour l'exercice de la liberté d'expression et d'opinion à travers le monde est en train de se constituer ; une véritable agora mondiale à laquelle participeront, en 2015, trois milliards et demi de personnes - la moitié de l'humanité !* »

« *Pour les peuples opprimés, pour tous ceux que les régimes autoritaires privent du droit de s'exprimer et de décider de leur avenir, ce réseau est devenu un outil de résistance irremplaçable et porteur d'espoir. Un seul exemple, parmi tant d'autres : l'Iran. Après les élections présidentielles de 2009 et la répression qui a suivi, Internet a été un relais essentiel, un catalyseur pour l'opposition démocratique au point que Shireen Ebadi a proposé de décerner à l'Internet le Prix Nobel de la Paix.* » Le rôle joué notamment par *Twitter* dans la contestation de la réélection de Mahmoud Ahmadinejad en Iran, eut en effet pour le monde entier valeur de symbole, le réseau social ayant permis aux manifestants iraniens de contourner la censure, de rester en contact les uns avec les autres, d'organiser des manifestations en faveur de Mir Hussein Moussavi, de faire connaître son visage au monde entier et de témoigner enfin d'événements auxquels les médias traditionnels n'avaient pas accès.

Plus récemment, le rôle d'Internet dans les événements qui ont conduit à la chute de plusieurs régimes dans le monde arabe a également été amplement souligné mais son importance réelle fait l'objet de nombreux débats.

Dans un ouvrage intitulé *The Net delusion : the Dark Side of Internet Freedom* (*L'illusion du Net : la face obscure de la liberté sur Internet*), Evgueny Morozov dénonce la « cyberutopie », qui attribue à la technologie des vertus émancipatrices intrinsèques, tout en refusant obstinément de prendre en considération ses aspects négatifs.

Il importe de ne pas surestimer ni sous-estimer le rôle d'Internet dans ces événements.

Bien sûr, il va sans dire que ce n'est pas Internet et les réseaux sociaux qui font la révolution, les expressions « webrévolution » ou « révolution 2.0 » étant assurément à cet égard un abus de langage. Les immolations publiques, les manifestations interdites ou l'occupation de la place Tahrir sont avant tout des expressions physiques d'un désarroi et d'une contestation populaires, face à des régimes autocratiques.

Comme le souligne Pierre Haski dans un article publié dans *Rue 89* le 22 janvier 2011, le geste de Mohamed Bouazizi, l'homme qui s'est immolé à Sidi Bouzid, déclenchant le processus qui a abouti un mois plus tard à la fuite du dictateur tunisien, n'a évidemment pas été déclenché par Internet, mais par sa propre exaspération face à l'arbitraire dont il avait été victime. « *Mais là où cet événement aurait pu rester localisé et ignoré, il a circulé et a mis le feu à la Tunisie. Et le vecteur de la circulation de l'info fut Internet ou, pour être plus précis,* Facebook*, qui, avec 2 millions de comptes en Tunisie, était devenue la seule plateforme d'échange d'informations non censurée du pays, alors que* YouTube *ou* Twitter *étaient devenus inaccessibles.* Facebook *était devenu un « territoire libéré » pour les jeunes Tunisiens urbains, un pays virtuel où se disait et se montrait tout ce qui pouvait déplaire au régime de Ben Ali. Lorsque les premières images de manifestations et de répression ont commencé à circuler, elles ont trouvé sur* Facebook *le vecteur idéal. Ces images ont sans doute représenté le point de non-retour pour cette crise sociale devenue révolution politique, et c'est incontestablement l'effet* Facebook. »

B. LES LIMITES À LA LIBERTÉ D'EXPRESSION ET DE COMMUNICATION SUR INTERNET

1. Les limites fixées par le droit

Sur Internet comme sur tout autre support, la liberté d'expression et de communication ne saurait être une liberté absolue. C'est pourquoi, fondamentale, elle est néanmoins une liberté dont la proclamation s'accompagne immanquablement de limitations, en tout cas dans la tradition juridique européenne en général, et française en particulier, comme en témoigne la formulation de l'article 11 de la Déclaration des droits de l'homme et du citoyen. Le respect dû à cette liberté n'implique pas d'autoriser la diffamation, l'atteinte à la dignité des déportés par des messages à caractère révisionniste ou encore la mise en scène pornographique d'enfants.

Lors de son audition du 27 octobre 2010, M^{e} Olivier Schnerb, avocat à la cour d'appel de Paris, a rappelé que les propos qui étaient échangés sur *Facebook* tombaient sous le coup de la loi. Une personne qui au cours d'une réunion dit du mal de quelqu'un, sous forme d'injure ou de diffamation, peut être poursuivie devant le tribunal de police ou devant le tribunal correctionnel si l'assemblée est

nombreuse. Il n'y a aucune raison que le tchat, le twit ou *Facebook* soient à l'abri de ces poursuites ordinaires.

Des limitations peuvent également viser à protéger d'autres droits fondamentaux, tels que le droit à la vie privée et le droit de propriété intellectuelle.

Si les caractéristiques d'Internet ont démultiplié la liberté d'expression et de communication, elles rendent également plus difficile la répression de ses abus. Comme l'a constaté le rapport de M. Christian Paul, *Du droit et des libertés d'Internet*, remis au Premier ministre le 29 juin 2000, « *l'Internet pose au droit des problèmes nouveaux et multiples* ». La lutte contre les contenus illicites se heurte en effet non seulement aux caractéristiques techniques inhérentes au réseau (transfrontalisme, volatilité des contenus...) mais aussi à la diversité des conceptions de la liberté d'expression dans les différents États. Le contenu d'un message transporté sur Internet peut être jugé innocent ici, indécent là et criminel ailleurs. Effectivement, la pornographie par exemple, interdite en Irlande, sanctionnée par des coups de fouet en Arabie Saoudite, est totalement libre en Suède. Dans certains pays anglo-saxons, les discours d'incitation à la haine raciale (néo-nazis) sont tolérés au nom de la liberté d'expression alors qu'ils sont poursuivis au pénal en France car attentatoires à la dignité humaine, au nom du même principe.

Lors de son audition du 16 juin 2010, M. Jean-Michel Quillardet, membre de la Commission nationale consultative des droits de l'homme (CNCDH), a indiqué à la mission que cette commission avait rendu plusieurs avis importants sur ces questions. Dans celui du 14 novembre 1996, elle a défendu la position selon laquelle la liberté d'expression sur Internet devait bénéficier des mêmes garanties que celles qui lui sont reconnues sur les médias traditionnels. Ainsi, de même qu'un directeur de publication voit sa responsabilité engagée en cas de diffamation, le propriétaire d'un site Internet doit être responsable du contenu qu'il héberge, sous réserve qu'il ait connaissance du fait diffamatoire. La CNCDH a également rappelé, dans cet avis, la nécessité de lutter contre la publication des propos racistes, antisémites et xénophobes sur Internet. Pour mieux connaître ce phénomène, elle a proposé la création d'un observatoire national, qui aurait eu aussi un rôle de médiation. Elle a, en outre, suggéré l'élaboration d'un code de déontologie, en particulier pour mieux protéger le droit d'auteur.

La question des modalités de la lutte contre les contenus illicites sur Internet est abordée plus précisément dans la première partie du titre III du présent rapport consacrée à la neutralité de l'Internet.

2. La censure imposée par certains États

Selon un rapport publié le 11 mars 2011 par Reporters sans frontières (RSF), le nombre de pays qui pratiquent la censure, en usent pour surveiller et punir pour délits d'opinion, progresse à un rythme inquiétant. RSF considère que près d'un internaute sur trois dans le monde a accès à un Internet censuré.

Or, le réseau des réseaux, lorsqu'il n'est plus un espace de liberté, peut se transformer, comme tout média, mais avec une puissance décuplée, en instrument de propagande, de désinformation, de répression et de surveillance.

L'association dresse ainsi une liste de dix pays qui tentent de contrôler les contenus sur Internet, en pratiquant la censure, la répression physique des acteurs du Net ou en ayant recours à la diffusion de messages de propagande.

Trois pays se distinguent par le nombre de blogueurs ou de « net-citoyens » emprisonnés : la Chine, tout d'abord, où 77 d'entre eux, dont le Prix Nobel de la paix, Liu Xiaobo, sont sous les verrous ; le Vietnam, avec 17 blogueurs emprisonnés ; l'Iran, où onze internautes sont détenus. La répression est particulièrement sévère dans ce pays où le blogueur irano-canadien Hossein Derakhshan a été puni d'une peine de dix-neuf ans de prison. Au total, 119 cyberdissidents sont ainsi privés de liberté dans le monde.

Les autres pays placés par RSF sur la liste noire sont l'Arabie saoudite, la Birmanie, la Corée du Nord, Cuba, l'Ouzbékistan, la Syrie et le Turkménistan.

Selon M. Olivier Esper, chargé de relations institutionnelles de la société *Google France*, entendu par la mission le 8 septembre 2010, la liberté d'expression, qui a connu une expansion importante grâce à Internet, est néanmoins fragilisée par l'action de certains pays autoritaires qui y voient une menace. La société *Google* s'est fermement engagée à préserver la liberté d'expression des internautes. Cette politique trouve son illustration dans l'évolution des relations liant la société *Google* à la Chine. Si, pendant quelques années, la société *Google* a accepté de censurer certains sites considérés par les autorités chinoises comme contrevenant à leurs règles, elle a mis un terme à cette pratique depuis février 2010, permettant ainsi à chaque internaute chinois d'avoir accès à la totalité des données et informations présentes sur le Web. La société *Google* procède également, chaque semestre, dans un souci de transparence envers les internautes, à la publication de l'ensemble des demandes émanant d'autorités étatiques visant à la suppression de contenus. De même, elle participe au programme « *Global Network Initiative* », plateforme commune à diverses entreprises et ONG, qui lutte contre le dévoiement des nouvelles technologies utilisées à des fins de répression et définit une position commune face aux régimes autoritaires. Une telle approche a reçu le soutien de diverses personnalités telles que la Secrétaire d'État américaine, Mme Hillary Clinton. Dans la même perspective, *Google* participe au travail engagé par M. Bernard Kouchner visant à mieux garantir la liberté d'expression au plan international.

Il convient de relever que le rapport de RSF met également sous surveillance seize pays, dont, pour la première fois, la France, où l'association souligne les risques que feraient, selon elle, peser sur la liberté d'expression les lois « Hadopi » [(1)] et la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, qui prévoit une possibilité de blocage administratif de l'accès aux sites pédopornographiques, sans décision de justice préalable. RSF estime qu'une fois ce cap « psychologique » franchi, un certain nombre d'autres raisons peuvent être utilisées pour bloquer l'accès à d'autres sites Internet. Les enjeux et éléments du débat relatif au blocage de l'accès à certains sites seront précisés dans la première partie du titre III du présent rapport consacrée à la neutralité du net.

Les participants de la réunion consacrée à Internet et la liberté d'expression qui s'est tenue le 8 juillet 2010 au ministère des Affaires étrangères et européennes avaient également constaté le nombre croissant d'atteintes à la liberté d'expression sur Internet dans le monde et engagé, pour y faire face, des travaux dans quatre directions :

– la mise en place, au niveau international, d'un mécanisme d'observation en matière de liberté d'expression et d'opinion sur Internet. Fédérant l'ensemble des initiatives prises dans ce sens, notamment par les acteurs de la société civile, il permettrait de constituer un groupe de pression suffisamment puissant pour interpeller les États qui manquent à leurs engagements ;

– l'élaboration d'un code de bonne conduite auquel les entreprises privées exportatrices de technologies de filtrage et de brouillage pourraient souscrire pour renforcer leur responsabilité face aux risques de détournement de leurs technologies par des régimes autoritaires ;

– l'aide aux défenseurs des droits de l'homme et aux cyberdissidents, qui doivent bénéficier du même soutien que les autres victimes de répression politique ;

– une réflexion sur les moyens de donner une traduction juridique à l'universalité d'Internet et lui conférer un statut qui le rapproche d'un espace international afin de contrecarrer ceux qui utilisent l'argument de la souveraineté contre les libertés fondamentales. Il s'agit là d'un travail de longue haleine sur lequel le Conseil de l'Europe et M. Franck La Rue, rapporteur spécial de l'ONU pour la liberté d'expression, ont engagé une réflexion.

En juin 2011, le rapporteur spécial des Nations unies pour la protection de la liberté d'expression a publié un rapport qui souligne l'importance démocratique vitale prise par Internet, et s'oppose à sa censure arbitraire et à sa surveillance généralisée. Le rapport en conclut notamment que la suspension de l'accès à

(1) Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet et loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet.

Internet est illégale au regard du droit international. « *Couper des utilisateurs de l'accès à Internet, quelle que soit la justification avancée, y compris pour des motifs de violation de droits de propriété intellectuelle, est* » selon le rapporteur spécial « *disproportionné et donc contraire à l'article 19, paragraphe 3, du Pacte international relatif aux droits civiques et politiques*. » 41 pays, parmi lesquels on peut relever que la France ne figure pas, ont approuvé les conclusions du rapport.

II. L'ACCÈS À L'INFORMATION DANS L'UNIVERS NUMÉRIQUE

Les sociétés de l'ère numérique sont traditionnellement présentées comme des « sociétés de l'information » ou des « sociétés de la connaissance », caractérisées par une forte diffusion des flux de données entre acteurs. Qu'en est-il du développement l'information en ligne et dans quelles mesures change-t-il la façon dont les individus ont accès à l'information ? Quels en sont les bénéfices et les risques pour l'information du citoyen ?

A. INTERNET AU SERVICE DE L'INFORMATION DU CITOYEN

Internet constitue incontestablement un vecteur d'accès à des sources sans cesse plus riches et nombreuses d'informations pour tous, et pas seulement pour les journalistes. Il permet la révélation de faits auxquels les médias traditionnels n'avaient pas accès ou que, parfois trop prudents ou pusillanimes, ils s'interdisaient de publier.

Avec une rapidité que ne permettaient pas les médias traditionnels, certains témoignages peuvent être apportés par des amateurs, depuis l'atterrissage d'un avion civil sur le fleuve Hudson (1) jusqu'à la mort d'Oussama Ben Laden.

Internet offre également à chacun la possibilité de s'exprimer, à travers notamment les réseaux sociaux, *Twitter* étant par exemple devenu un indicateur des sujets de préoccupation du jour, partout dans le monde.

Désormais, des sites Internet, des réseaux sociaux et des blogs, depuis le Drudge Report (2) jusqu'à *Twitter* et *Facebook* en passant par le Huffington Post (3), peuvent légitimement revendiquer le statut de média d'information.

---

*(1) Le 15 janvier 2009, un Airbus réalisait un amerrissage d'urgence dans le fleuve Hudson à New York ce qui a permis de sauver les 155 passagers du vol 1549 de l'*US Airways*. Quelques minutes plus tard, des vidéos et photos amateurs de l'événement étaient postées sur Internet.*

(2) Le Drudge Report*, lancé en 2007 par l'Américain Matt Drudge, constitue le plus célèbre exemple d'une nouvelle manière d'informer qui s'est répandue sur Internet : le journalisme de liens, qui consiste à sélectionner des liens hypertextes vers des pages web affichant des informations jugées pertinentes sur un sujet donné. Ce site séduit par sa simplicité près de 12 millions de visiteurs uniques par mois. Engagé politiquement, il dresse des listes thématiques de liens et ne produit aucun contenu.*

(3) Lancé en 2005 par l'éditorialiste américaine Arianna Huffington, ce site d'information généraliste attire plus de 25 millions de visiteurs uniques par mois, une audience supérieure à celle des grands quotidiens américains tels que le Washington Post *(16,2) et le* Wall Street Journal *(12,2).*

L'élection de Barack Obama en novembre 2008, les manifestations en Iran au printemps 2009 et les récents événements qui ont secoué le monde arabe ont donné aux réseaux sociaux leurs lettres de noblesse. Ils sont devenus des moyens d'information à part entière, ce qu'ils étaient déjà, au moins aux yeux de la génération numérique née après 1985 et plus encore parmi les plus jeunes, qui ont aujourd'hui moins de 15 ans. Ces événements ont prouvé que ces sites peuvent, dans certaines circonstances, contourner la censure et occuper la place des journalistes toujours moins nombreux à couvrir les crises internationales, pour des raisons qui sont non seulement politiques, mais également économiques.

WIKILEAKS ET LES MÉDIAS

En juillet 2010, un professionnel de l'informatique, Julien Assange, a défrayé la chronique après avoir mis en ligne sur son site, *WikiLeaks*, les « *war logs* », près de 77 000 documents secrets de l'armée américaine en Afghanistan. Parmi ces « *leaks* » (fuites), une vidéo intitulée « *Collateral Murder* » montrait des soldats américains tirant sur des civils irakiens et sur un journaliste de Reuters. Puis il annonça, sur ce même site, qui lui valut alors l'attention des grands médias de l'information planétaire, la parution prochaine de 13 000 nouveaux *war logs*.

WikiLeaks, fondé en 2007, avait déjà publié plusieurs milliers de documents fournis par des sources anonymes. Julien Assange se présente lui-même comme un pionnier d'une nouvelle forme de journalisme.

La plupart des publications de *Wikileaks* ont suscité de violentes polémiques. La démarche du site consistant à donner audience à des fuites d'information tout en protégeant ses sources est dénoncée par certains et louée par d'autres.

Quelle que soit la position que l'on peut avoir sur la vocation et les modalités d'action de *Wikileaks*, la mission estime, comme l'en a convaincu Robert D. Atkinson, président de l'ITIF (*Internet Technology ans Innovation Foundation*) rencontré par les rapporteurs lors de leur déplacement à Washington, que ce n'est pas le média Internet qui est en cause dans ce débat mais l'existence des fuites dont le site se fait l'écho, même si Internet facilite leur diffusion.

Le succès de *Wikileaks* est d'ailleurs largement imputable au fait que ses révélations ont été, à partir de juillet 2010, relayées par les grands médias traditionnels et notamment de grands quotidiens nationaux, comme le *New York Times*, *The Guardian, Le Monde, El Pais* et *Der Spiegel*, la synthèse de documents extrêmement lourds et techniques par ces médias permettant de conférer aux révélations un style journalistique plus facile à appréhender mais aussi d'occulter d'éventuelles mentions dangereuses pour des particuliers.

À cet égard, il est intéressant de constater que ceux qui ont pu préconiser la fermeture de *Wikileaks* n'ont pas appelé à une censure des grands médias traditionnels reprenant les informations divulguées par le site.

Le numérique est également un atout dont doit se saisir la presse traditionnelle.

Aujourd'hui, les journalistes ne se contentent plus d'informer : ils sont aussi amenés à communiquer. Tous les sites d'information proposent des outils de partage, accolant à leurs articles le « tag » de *Twitter* ou le « J'aime » de *Facebook*. Ainsi, les lecteurs-internautes sont invités à contribuer eux-mêmes de plus en plus à la propagation des informations avec les commentaires, posts, tags, twits... Comme ils ont su adopter la technique des 140 signes sur *Twitter* ou le post sur un mur *Facebook* afin d'assurer la notoriété de leurs reportages, les journalistes se transforment également en animateurs de communautés

d'internautes ou en modérateurs afin d'être au plus près des préoccupations des lecteurs.

Parmi les incontestables apports du Web à la presse traditionnelle, figure le « *rich média* » qui consiste à enrichir l'écrit d'images, de sons, de vidéos et de graphiques. Les journalistes sont désormais « multisupports » et « multitâches ».

C'en est en outre fini de la pagination limitée. Le flux perpétuel des mises à jour remplace l'unique livraison en temps et en heure. Internet a imposé le temps réel, c'est-à-dire la diffusion directe et continue d'une multitude de flux d'informations. À l'ère du numérique, la consommation de l'information ne s'arrête jamais. Le temps est venu du « journal permanent », avec par exemple cinq éditions quotidiennes pour *Les Échos* sur iPad.

Comme la plupart des institutions, publiques ou privées, les célébrités comme les hommes politiques, en ont tiré la leçon : ils soignent leur réputation grâce à un profil *Facebook*, un compte *Twitter*, l'affiliation à un réseau professionnel LinkedIn ou le français *Viadeo* et surveillent leurs fiches sur *Wikipédia* ou *Google*. Ils y trouvent l'occasion de « communiquer » directement, court-circuitant ainsi les médias traditionnels, lorsqu'il ne s'agit pas tout simplement de prendre la parole dans un débat auquel ils ne sont pas conviés.

B. INTERNET : MENACE POUR L'INFORMATION DE QUALITÉ ?

Que serait cette galaxie d'informations diffusées sur Internet, sans le relais amplificateur des grands médias traditionnels ? Que vaudrait surtout l'information en provenance du Web 2.0 sans le filtre, les analyses et les commentaires des experts et des journalistes qualifiés ?

Internet est capable, comme toute autre technique, du meilleur comme du pire. En étant le plus puissant instrument de communication jamais inventé par l'homme, Internet peut aussi se révéler un redoutable outil de désinformation.

En multipliant les espaces de conversations, le Web 2.0 est, plus que les autres médias, un lieu d'où partent et se diffusent des informations fabriquées, comme récemment la photographie truquée du corps d'Oussama Ben Laden, et les rumeurs et théories les plus fantasques et dévastatrices, telles que l'idée selon laquelle Barack Obama était en réalité Oussama Ben Laden... Internet offre la possibilité de recourir à diverses techniques de désinformation, telles que l'« *astroturfing* », qui s'appuie sur des internautes complices pour lancer des rumeurs malveillantes, ou le « *spamdexing* », procédé de référencement abusif visant à augmenter le nombre de liens vers un site déterminé.

La propagation virale de rumeurs dans les réseaux sociaux est d'autant plus efficace, en l'occurrence, que l'on se fie plus volontiers à ses proches, à ceux que l'on croit proches, amis ou « suiveurs », qu'aux médias traditionnels qui voient leur crédibilité baisser d'année en année. C'est ce qu'ont démontré

récemment Mme Josiane Jouët, qui dirige le centre d'analyse et de recherche interdisciplinaire sur les médias (CARISM) et M. Thierry Vedel, du Centre de recherches politiques de Science Po (CEVIPOF), dans le cadre d'une enquête auprès de 1 800 Français de plus de 15 ans. Le danger est d'autant plus grand que les 15-25 ans sont les plus nombreux parmi les 80 % des 35 millions d'internautes français à être connectés à au moins un réseau social.

C'est pourquoi la mission estime que l'avenir du journalisme et de la presse professionnels doit être un sujet de préoccupation majeur pour les pouvoirs publics. Car la fragilisation et l'éventuelle disparition des médias traditionnels de l'information, qui pourrait résulter de l'essor d'Internet, constituent un risque réel de perte de l'un des fondements des sociétés démocratiques.

Un rapport de l'Organisation de coopération et de développement économique (OCDE) intitulé *L'avenir de l'information et d'Internet* de juin 2010 décrit et analyse la crise de l'industrie de la presse dans le monde. Cette dernière touche l'ensemble des pays développés, où les entreprises de presse, subissent une baisse très inquiétante de leurs revenus tirés de la publicité et de leur diffusion. Environ 20 pays sur les 31 étudiés ont subi une baisse de leur lectorat, liée notamment à la désaffection des jeunes pour le média imprimé au profit d'Internet.

La mauvaise conjoncture économique a certes contribué à amplifier le déclin progressif du marché de la presse écrite, mais le principal défi auquel il est confronté réside dans son adaptation au numérique et à l'arrivée sur le marché de l'information de nouveaux acteurs comme les portails Internet, les agrégateurs de contenus, les éditeurs de presse en ligne *(pure players),* les applications pour *smartphones* et autres tablettes numériques, le journalisme citoyen, les réseaux sociaux et les services de communication comme *Twitter*, qui sont autant de concurrents pour la presse traditionnelle.

Si la lecture de la presse en ligne est une activité en pleine croissance sur Internet, elle n'a encore pas trouvé de modèle économique viable. Une moyenne de 20 % de la population lit les journaux en ligne dans les pays de l'OCDE, 57 % aux États-Unis et seulement 22 % en France. Les deux tranches d'âge les plus attirées par la lecture des informations en ligne sont les 16-24 ans et, plus encore, les 25-34 ans. Néanmoins, leur disposition à payer pour avoir accès à des informations en ligne est faible. En outre, la lecture sur Internet est plus occasionnelle et plus souvent déclenchée par un événement particulier que celle de la presse traditionnelle. Parallèlement, les revenus de la publicité en ligne, qui ne représentent que 4 % du chiffre d'affaires de la presse en 2009, constituent une ressource encore infime pour les journaux.

Avec Internet, de nouveaux modèles économiques ont été expérimentés comme des formules de paiement à l'acte ou de forfait dans un premier temps, puis, dans un second temps, à la fin de l'année 2009, des offres de contenus en ligne spécifiques dits « premium », les éditeurs comptant sur une plus grande

disposition de leurs lecteurs à payer pour une information de qualité. À l'exception de quelques titres, les revenus supplémentaires sont restés négligeables. Aucun modèle économique n'a donc encore été trouvé pour financer durablement une production professionnelle et indépendante d'informations, ce qui pose le problème de la viabilité d'un journalisme de qualité à long terme.

LES FERMES DE CONTENUS

Dans un article publié dans le numéro hiver 2010-2011 de la *Revue européenne des médias*, « Journalisme, quels métiers ! », Mme Françoise Laugée fait le point sur l'influence que pourrait avoir sur l'information cette production de contenus d'un genre nouveau, qui sonde les requêtes des internautes afin de déterminer les sujets les plus en vogue sur le Net et d'y associer des messages publicitaires. Ainsi, des milliers de contenus, articles, billets ou vidéos, sont-ils produits en fonction de l'analyse de millions de mots clés faisant émerger les thèmes les plus populaires.

Nées aux États-Unis, ces nouvelles plates-formes de contenus à la demande, également appelées « fermes de contenus », emploient des rédacteurs indépendants, parmi lesquels des journalistes professionnels, pour rédiger des articles faisant figurer, au moins dans le titre si ce n'est pas dans le corps du texte, un mot-clé plébiscité. Leur mode de rémunération se fait à l'article et varie selon les sites. Généralement composée d'une partie fixe et d'un intéressement aux recettes publicitaires générées, la rémunération est parfois calculée exclusivement sur le nombre de clics effectués par les internautes sur les liens publicitaires. Les gains sont toutefois modestes, en moyenne de 5 à 15 euros par article. Ces fermes de contenus fournissent essentiellement des informations d'ordre général sous la forme de fiches ou d'articles conseils. La plupart des dirigeants de ces « usines à infos » se défendent de traiter l'actualité et revendiquent leur place sur le marché de l'information pratique : finance, voyage, cuisine, bricolage, médecine... En s'appuyant sur les données statistiques des sujets déjà largement traités sur le Net, les fermes de contenus cherchent davantage à attirer les annonceurs en quête d'une large audience qu'à informer les internautes. Néanmoins, des sites d'information générale et politique pourraient être attirés par cette formule en privilégiant les sujets favoris des internautes afin d'augmenter leurs revenus publicitaires. Le blog *Upshot* consacré à l'actualité est le premier du genre.

Cette pratique, si elle se répandait, ne serait pas sans risque pour la crédibilité des médias d'information générale et politique. La production de contenus à la demande est une activité en pleine croissance. Même si le modèle n'est pas encore rentable, le phénomène est en train de prendre de l'importance sur Internet, et pas seulement pour les consommateurs américains.

Le risque, estime Mme Françoise Laugée, serait que l'information de qualité soit réservée à une élite d'abonnés payants, tandis qu'une information *low cost* serait diffusée gratuitement au plus grand nombre selon la logique des algorithmes censés refléter les attentes de la population en matière d'information.

C. DES MESURES EN FAVEUR D'UNE INFORMATION DE QUALITÉ À L'ÈRE NUMÉRIQUE

1. Les mesures mises en place

À court terme, les pays de l'OCDE ont mis en place des mesures d'urgence pour aider financièrement l'industrie de la presse en difficulté, au premier rang desquels se trouve la France. Notre pays, à l'issue des états généraux de la presse écrite, qui avaient été lancés en octobre 2008, a décidé de consacrer une aide exceptionnelle d'un montant de 600 millions d'euros sur trois ans à un plan de modernisation de la presse écrite (sans compter les coûts de restructuration dans les imprimeries afin d'obtenir des gains de productivité). Le montant total

des aides de l'État à la presse s'élève désormais en France à 1,2 milliard d'euros en 2010, ce qui représente plus de 12 % du chiffre d'affaires du secteur.

Au contraire, aux États-Unis**,** le gouvernement a décidé qu'il n'y aurait pas de plan de sauvetage pour la presse américaine, alors que certaines grandes villes n'auront bientôt plus de quotidien local et que, depuis janvier 2008, 67 journaux américains ont disparu et sept groupes de presse ont cessé leur activité. Lors d'une réunion de la sous-commission sénatoriale des communications, de la technologie et de l'Internet, son président John Kerry a ainsi qualifié les journaux « *d'espèce en danger* ».

En France, diverses mesures ont été prises afin d'aider la presse dans la nécessaire mutation que lui impose la révolution numérique. La loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet a introduit une définition des services de presse en ligne [(1)] qui permet à ces derniers d'accéder partiellement au régime économique des aides à la presse : possibilité de constituer des provisions pour investissement, exonération de la contribution économique territoriale et accès à un nouveau fonds d'aide au développement des services de presse en ligne (fonds SPEL), créé pour une durée de trois ans et doté de 20 millions d'euros par an sur trois ans.

Lors de son audition par M. Michel Françaix, rapporteur pour avis des crédits en faveur de la presse au nom de la commission des Affaires culturelles et de l'éducation dans le cadre du projet de loi de finances pour 2011, M. Bruno Mettling, inspecteur général des finances chargé par le Gouvernement d'un rapport sur l'efficacité des aides à la presse, a déploré que l'on ait ainsi mobilisé une enveloppe considérable de 20 millions d'euros, sans aucune réflexion préalable, ni sur son montant, ni sur son ciblage, l'économie de la presse en ligne présentant la particularité de ne comporter aucune barrière à l'entrée.

Il en résulte, selon lui, un guichet supplémentaire et un saupoudrage inéluctable des crédits. Le fonds n'est pas ciblé sur la presse d'information politique et générale. Son articulation avec le fonds d'aide à la modernisation de la presse quotidienne et assimilée d'information politique et générale (FDM), qui permet d'accorder des subventions aux entreprises et agences de presse pour la réalisation de projets de modernisation, n'est par ailleurs pas claire : certaines aides qui n'ont pu être distribuées dans le cadre du FDM l'auraient été par le fonds SPEL. Dans le cadre de la réforme annoncée des modalités du soutien de l'État en faveur de la presse, il conviendra d'apporter les ajustements qui s'imposent afin de mieux aider la presse à se développer dans l'univers numérique.

---

(1) « On entend par service de presse en ligne tout service de communication au public en ligne édité à titre professionnel par une personne physique ou morale qui a la maîtrise éditoriale de son contenu, consistant en la production et la mise à disposition du public d'un contenu original, d'intérêt général, renouvelé régulièrement, composé d'informations présentant un lien avec l'actualité et ayant fait l'objet d'un traitement à caractère journalistique, qui ne constitue pas un outil de promotion ou un accessoire d'une activité industrielle ou commerciale*. ».*

La loi favorisant la diffusion et la protection de la création sur Internet précitée a également mis en place un nouveau cadre juridique pour la gestion des droits d'auteur des journalistes qui remplace un droit lié à la publication sur un support par un droit lié à un temps d'exploitation afin de favoriser l'exploitation plurimédia d'un même article.

Enfin, un engagement de développement de l'emploi et des compétences a été conclu le 30 juin 2009, pour trois ans, entre les partenaires sociaux de la presse écrite et le secrétaire d'État à l'Emploi et a pour objectif de réduire la fracture numérique au sein des entreprises de presse, quel que soit l'emploi occupé. Il s'agit de contribuer à adapter la formation de tous les salariés participant à la création et à la promotion d'un titre de presse aux nouvelles technologies liées au numérique.

2. Les chantiers ouverts

La baisse du taux de la TVA applicable à la presse en ligne demeure un chantier majeur et prioritaire des pouvoirs publics pour favoriser le développement ou la survie de la presse sur Internet. Rappelons qu'en l'état actuel, la presse en ligne est soumise à un taux de 19,6 % alors que la presse imprimée bénéficie d'un taux super-réduit de 2,1 %, le droit de l'Union européenne ne permettant pas qu'un taux réduit ou super-réduit de TVA soit appliqué aux publications de presse en ligne [(1)].

À l'heure où l'équation économique de la presse en ligne se cherche encore, le secteur s'accommode difficilement d'une fiscalité alourdie par rapport à la presse papier. Aussi le Gouvernement souhaite-t-il pouvoir remédier à cette situation en obtenant une modification du droit européen. Des discussions en ce sens sont engagées depuis 2006, la révision éventuelle des structures des taux de TVA devant s'effectuer à l'unanimité des États membres du Conseil.

Le dossier a connu un début d'évolution depuis qu'un amendement au projet de loi de finances pour 2011 a été adopté afin de fixer le taux de la TVA sur le livre numérique à 5,5 % à compter du 1er janvier 2012 au nom d'une « certaine exception française en matière culturelle ».

---

(1) Les modalités selon lesquelles les États membres de l'Union sont autorisés à fixer le taux applicable aux opérations assujetties à la TVA sont déterminées par la directive 2006/112/CE du Conseil du 28 novembre 2006 (« directive TVA »). Les paragraphes 1 et 2 de l'article 98 de cette directive prévoient que soit un, soit deux taux réduits, qui ne peuvent être inférieurs à 5 %, peuvent être appliqués aux livraisons de biens et aux prestations de services des catégories limitativement énumérées en son annexe III. C'est sur ce fondement, combiné avec une disposition transitoire permettant le maintien des taux inférieurs à 5 % qui préexistaient à l'établissement, en 1992, de la liste reprise dans l'annexe III, que le taux de 2,1 % est aujourd'hui appliqué en France métropolitaine aux opérations de « ventes, commissions et courtages portant sur les publications qui remplissent les conditions prévues par les articles 72 et 73 de l'annexe III du présent code » (article 298 septies *du code général des impôts). Ce taux super-réduit constitue l'une des principales mesures du régime économique de la presse écrite. En revanche, si l'annexe III de la directive TVA mentionne bien les « journaux et périodiques », elle ne vise que les publications imprimées et non celles sur support électronique. Ces règles, sans équivoque, ne permettent pas d'assimiler une publication en ligne à un journal ou à un périodique imprimé pour le bénéfice du taux super-réduit de TVA de 2,1 %.*

À la suite de l'adoption de cet amendement, le Président de la République a confié à M. Jacques Toubon une mission visant à recueillir les propositions et les positions tant de la Commission européenne que des 27 États membres de l'Union européenne sur la différence des régimes fiscaux applicables aux biens culturels, *y compris la presse*, selon qu'ils sont matériels ou dématérialisés.

Les états généraux de la presse écrite ont également ouvert un chantier sur la réforme du système d'aides à la presse, sujet sur lequel une mission a été confiée à M. Aldo Cardoso. Ce dernier a proposé une réforme globale des modalités d'intervention de l'État en matière d'aides à la presse. Il souhaite notamment que les aides soient réorientées en vue de soutenir de véritables stratégies d'investissement : encourager l'innovation, le renouvellement de l'offre, les stratégies de diversification plurimédia, les laboratoires et incubateurs d'innovation portés par des associations professionnelles afin de pallier les carences du système français en matière de mutualisation des coûts de recherche et développement. Cette réorientation de l'effort financier de l'État est de nature à améliorer le soutien à la nécessaire adaptation de la presse à l'univers numérique.

La mission se félicite également des initiatives prises par les acteurs du secteur pour mutualiser leurs moyens et favoriser l'émergence de kiosques numériques payants. De grands acteurs de la presse quotidienne nationale (*Libération, Le Figaro, L'Équipe, Les Échos, Le Parisien*), rejoints par plusieurs magazines (*l'Express, le Point, le Nouvel Observateur*), ont par exemple annoncé la création d'un groupement d'intérêt économique (GIE) en vue de mettre en place un portail commun de la presse en ligne.

Cette initiative est destinée à contrer l'agrégateur « *Google Actualités* », qui, selon les titres de la presse, pratique « une forme de parasitisme économique », en présentant le meilleur de chaque titre, ce qu'aucun éditeur ne peut proposer individuellement. Ainsi « *Google Actualités* » a-t-il réussi à se positionner comme site de référence de l'accès à l'information, et ceci sans verser de contrepartie financière aux journaux qui supportent les coûts de la création d'une information de qualité.

Il est donc très important, comme l'a souligné l'Autorité de la concurrence dans son avis du 14 décembre 2010, que les éditeurs de presse puissent demander et obtenir d'être exclus de « *Google Actualités* » sans pour autant être déréférencés du moteur de recherche de *Google*. L'entreprise a pris des engagements en ce sens devant l'autorité de concurrence italienne : l'indexation des contenus de presse dans « *Google Actualités* » doit être découplée – par une démarche simple et préalable des éditeurs – de celle des contenus accessibles grâce au moteur de recherche généraliste. L'Autorité de la concurrence française devra veiller à ce que ces engagements, que *Google* annonce avoir déjà mis en œuvre, soient respectés en France.

Enfin, alors que l'arrivée des tablettes numériques, en particulier de l'*iPad*, était attendue par les fournisseurs de contenus numériques et les éditeurs

de presse comme « une planche de salut », voire un dernier espoir de monétiser l'information dans l'univers numérique, les conditions fixées par *Apple* en matière d'abonnements en février 2011 ont rapidement modéré leur enthousiasme.

Apple les autorisait à proposer des abonnements pour l'*iPhone* et l'*iPad* sur leur propre site Internet – c'est-à-dire en dehors d'*iTunes* et de l'*Apple Store*, à condition qu'ils proposent également dans ce cas un abonnement *via* l'*Apple Store*, à un prix égal ou inférieur à celui offert par ailleurs. Cette condition a été assouplie par *Apple* en juin 2010, le prix proposé directement par l'éditeur pouvant désormais être inférieur à celui de l'*Apple Store*. Les éditeurs pourront ainsi offrir des promotions ou répercuter sur le prix proposé *via* l'*Apple Store* la commission de 30 % prélevée par Apple. Il semblerait que les nombreuses réactions d'éditeurs auprès des autorités de la concurrence américaines ou européennes ont poussé *Apple* à faire évoluer sa position

Pour autant, ce geste consenti par Apple est loin de satisfaire les éditeurs de presse qui contestent le refus de la firme de leur communiquer les coordonnées de leurs clients via l'Apple Store, refus qui les prive de la relation commerciale avec leurs abonnés. Certes, Apple demande aux clients qui s'abonnent de donner leur accord pour que leurs coordonnées soient communiquées aux éditeurs, mais dans des termes bien trop dissuasifs, selon ces derniers. Les éditeurs contestent également la commission de 30 % des recettes générées via l'Apple Store, prélevée par Apple.

Orientation n° 1 : aider la presse d'information à se développer sur les nouveaux supports numériques

– clarifier et mieux cibler les aides attribuées dans le cadre du fonds d'aide au développement des services de presse en ligne (fonds SPEL) ;

– obtenir au plus vite l'autorisation d'appliquer un taux super-réduit de TVA à la presse en ligne ;

– dans le cadre de la réflexion sur une réforme globale des modalités d'intervention de l'État en faveur de la presse, s'assurer qu'un accent particulier soit porté sur le soutien à des stratégies d'investissement dans le développement numérique ;

– encourager les éditeurs de presse à développer *de façon concertée* des projets numériques permettant une meilleure valorisation de leurs contenus diffusés sur l'Internet et sur les plateformes mobiles ;

– s'assurer que *Google* respecte son engagement de permettre aux éditeurs de presse d'être exclus de « G*oogle Actualités* » sans pour autant être déréférencés du moteur de recherche ;

– charger l'Autorité de la concurrence d'examiner les pratiques d'*Apple* relatives à la vente d'abonnements à des titres de presse sur ses tablettes numériques (*Ipad*).

III. L'ACCÈS À LA CONNAISSANCE ET À LA CULTURE SUR LE WEB

L'article 27 de la Déclaration universelle des droits de l'homme de 1948 consacre un droit à la culture qui comprend plusieurs composantes : le droit de prendre part à la vie culturelle et de jouir des arts ; le droit de jouir des avantages du progrès scientifique et le droit de l'individu à bénéficier de la protection des intérêts moraux et matériels résultant de toute production scientifique, littéraire ou artistique dont il est l'auteur.

Le droit à la culture et à la connaissance comporte également le droit de s'assurer que la culture et la connaissance sont conservées, développées et diffusées. Les obligations des États de respecter et de protéger le patrimoine culturel ont particulièrement été renforcées à travers des traités adoptés sous les auspices de l'UNESCO (Organisation des Nations unies pour l'éducation, la science et la culture).

Or, si les technologies de l'information et de la communication contribuent de façon spectaculaire au développement de l'accès à la connaissance et à la culture, dans leur acception la plus extensive, elles ne vont pas sans soulever de nombreuses interrogations sur ses modalités, la répartition des rôles entre acteurs privés et publics et les menaces éventuelles que le numérique pourrait faire peser sur les médias traditionnels et la production de contenus.

A. LE NUMÉRIQUE : VECTEUR DE DÉMOCRATISATION ET D'ÉVOLUTION DES MODES D'ACCÈS AU SAVOIR ET À LA CULTURE

Le numérique redéfinit de façon radicale les modes d'accès au savoir et à la culture : à des relations verticales entre leurs détenteurs et leurs destinataires se substituent des relations horizontales où chacun devient potentiellement émetteur et récepteur de données. La démocratisation de l'accès à la connaissance, à l'information et à la culture qui en résulte est comparable, par son ampleur, aux ruptures qui ont marqué diverses périodes historiques : la Renaissance avec le développement de l'imprimerie ou les Lumières et le XIX^{e} siècle avec le développement de la presse écrite.

1. La décentralisation des savoirs

La société engendrée par ce nouveau saut technologique a été abondamment étudiée par les philosophes et les sociologues, du fait des changements de conception du monde, voire des modes de pensée, qu'elle induit et de la « décentralisation des savoirs » qu'elle implique.

L'auteur et journaliste américain Nicholas Carr, pourtant très critique sur les effets d'Internet sur les modes de penser, dans un article intitulé « *Google* nous rend-il idiots ? » [(1)] explique qu'en tant qu'écrivain, il a reçu le web comme une bénédiction. « *Les recherches, autrefois synonymes de journées entières au milieu*

(1) Internet : la révolution de savoirs, *novembre 2010, La Documentation française.*

des livres et magazines des bibliothèques, s'effectuent désormais en un instant. Quelques recherches sur Google*, quelques clics de lien en lien et j'obtiens le fait révélateur ou la citation piquante que j'espérais. Même lorsque je ne travaille pas, il y a de grandes chances que je sois en pleine exploration du dédale rempli d'informations qu'est le web ou en train de lire ou écrire des e-mails, de parcourir les titres de l'actualité et les derniers billets de mes blogs favoris, de regarder des vidéos et d'écouter des podcasts ou simplement de vagabonder d'un lien à l'autre, puis à un autre encore*. »

La part grandissante prise par les technologies numériques dans l'accès au savoir et donc dans l'éducation doit être ici soulignée. Que ce soit pour sélectionner l'information (à travers les bases de données numérisées ou les moteurs de recherche), acquérir les connaissances (avec les cours magistraux et les bibliothèques en ligne) ou pour les formaliser (au travers des logiciels de traitement de texte ou de présentation), leur apport à la construction du savoir au cours des processus d'apprentissage est aujourd'hui incontournable. C'est pourquoi, une politique ambitieuse d'éducation aux médias au sens large constitue une priorité, thème qui sera développé plus amplement dans la troisième partie du titre II du présent rapport.

Fondée en 2000 par les Américains Jimmy Wales et Larry Sang, *Wikipedia*, encyclopédie entièrement gratuite, créée par et pour les internautes, constitue sans doute l'un des meilleurs exemples de l'appropriation de l'accès au savoir par les internautes. En dix ans, l'encyclopédie gratuite et collaborative s'est imposée comme le site d'accès au savoir le plus visité au monde : en France, il rassemble environ 8 millions de visiteurs par mois, ce qui le place en dixième position, et bien évidemment en fait le premier site d'accès à la connaissance. Ce site a pourtant « mauvaise presse » dans la sphère publique française, et ce, alors il n'est probablement pas un internaute – même parmi ses détracteurs – qui n'y ait recours occasionnellement pour obtenir ou vérifier une information quelconque.

LE CAS *WIKIPÉDIA*

Sur *Wikipédia*, les articles ne sont pas signés par des experts, il n'y a pas d'architecture du savoir définie *a priori*, pas de clôture des connaissances « estampillée » par un comité d'experts. Chacun est libre d'éditer, de corriger et de modifier les contenus, participant ainsi à une vaste entreprise d'élaboration collective et de diffusion du savoir. Les volontaires sont invités à contribuer dans la mesure de leurs compétences – que ce soit en traduisant des articles, en réorganisant la structure d'un article, en ajoutant des illustrations, en corrigeant des fautes d'orthographe... Le collégien peut ainsi contribuer au projet, tout comme le professeur d'université.

« *Le principe de* Wikipédia*, c'est que plus il y a de contributeurs – plus les yeux sont nombreux –, plus une erreur a des chances d'être détectée* », selon Florence Devouard, ancienne présidente de la *Wikimedia Foundation* et membre du conseil d'administration de *Wikipédia* (1). « *C'est d'ailleurs souvent comme cela que l'on commence : un jour, on tombe sur un article comportant une erreur et on le modifie.* »

Le projet fait confiance à la base, au simple citoyen, selon le principe de l'information *bottom-up*, produite « du bas vers le haut », que beaucoup de « wikipédiens » considèrent comme complémentaire – voire plus fiable que l'information *top-down* (« du haut vers le bas ») des grands médias, suspectés d'avoir des intérêts particuliers à défendre.

(1) « Wikipédia*, révolution dans le savoir »,* La Croix, *8 mars 2011.*

L'encyclopédie, à but non lucratif, restée jusqu'à présent hostile à toute publicité en ligne, repose sur des milliers de bénévoles.

Il est vrai que si *Wikipédia* compte bien des avantages, à commencer par la masse d'informations qu'elle met gratuitement à la disposition de tous et sa réactivité, elle n'est pas sans présenter d'importantes limites.

Tout d'abord, « *il y a toujours une incertitude sur la qualité et pas de garantie en termes de résultat* », selon Mathieu O'Neil, maître de conférence à Paris IV, spécialiste des questions d'autorité et d'expertise sur le Net [(1)].

Par ailleurs, l'encyclopédie fonctionne en flux, son contenu n'est jamais fixé et peut toujours être modifié, ce qui est un avantage comme un inconvénient. « *Avec* Wikipédia*, on échange la garantie de fiabilité des encyclopédies classiques contre la gratuité et la possibilité d'un lien aux sources immédiates que* Wikipédia *impose à ses auteurs de citer* ».

Sur le fond, selon certains, la manière d'envisager le savoir peut aussi être questionnée, tout comme le principe de neutralité mis au fronton de l'édifice. «Wikipédia *revendique le «* no point of view » *(« l'absence de point de vue »). C'est une vision très rationaliste et même positiviste du savoir »,* selon Marc Foglia auteur de Wikipédia*. Média de la connaissance démocratique ?.* « *Comme l'esprit critique personnel ne peut pas s'exprimer, la vision des choses qui l'emporte est celle de la majorité. Les visions minoritaires sont éliminées*. »

Par ailleurs, des informations peuvent provenir de personnes et de sociétés qui instrumentalisent cet outil pour assurer leur propre publicité ou modifier anonymement les données objectives qui les concernent.

Dans un article publié dans la revue *Le Débat* [(2)], Pierre Assouline, très critique à l'égard de Wikipédia et de la « *grande illusion de la diffusion horizontale de la connaissance* » qui repose sur l'idée selon laquelle nous serions tous des experts, rapporte comment l'écrivain anglais Ben Myers a renoncé à se rendre dans le village de Roumanie où il avait situé une partie de son prochain roman. « *En une journée, il avait amassé toute sa documentation grâce à* Wikipédia *et même visualisé les rues grâce à* Google Earth. (…) » Et Pierre Assouline d'en conclure : « *J'ignore à quoi ressemblera son roman mais je sais ce qui lui manquera : l'imprégnation. Et cela, humer les rues, écouter les gens, observer les habitudes, noter les bruits, un écrivain ne peut l'obtenir par procuration car ça n'a pas sa place sur Internet.* » Certes, mais un voyage en Roumanie n'étant pas à la portée de chacun, il est appréciable que chacun soit en mesure de disposer des informations et images fournies par ces outils.

Au vu du rôle croissant de *Wikipédia* dans l'accès au savoir, des dangers multiples ont été annoncés, voire une véritable catastrophe pour la culture. On doit pourtant constater que cette dernière ne s'est pas produite.

Au contraire, selon Christian Vandendorpe [(3)], « *sans cet ouvrage de référence encyclopédique, on se retrouverait devant le chaos primitif du web de la fin des années 1990, où pullulaient les sites aux informations fantaisistes ou carrément biaisées, sur la véracité desquelles l'usager n'avait aucun moyen de contrôle une réalité souvent ignorée ou oblitérée par les détracteurs de* Wikipédia. »

Selon Christian Vandendorpe [(4)], « *les petites cultures ont trouvé dans ce nouvel espace un ballon d'oxygène et se font un point d'honneur de créer leur propre version : elles voient dans cette réalisation une façon d'affirmer publiquement leur existence et un espoir de renaissance de leur langue, qu'il s'agisse du wallon (9 346 articles), de l'occitan (10 418 articles), du breton (16 716 articles) ou du lingala (842 articles).* (…) *Étant totalement délocalisée,* Wikipédia *peut ainsi donner toute leur place à des personnages historiques considérés comme mineurs dans la sphère nationale dominante, mais importants pour une collectivité partageant la même langue. (…) »*

---

(1) Ibid.

(2) « Y a-t-il un bon usage de Wikipédia ? », Entretien avec Pierre Assouline, Le Débat, n° 148, janvier-février 2008.

(3) « Le phénomène Wikipédia : une utopie en marche », Christian Vandendorpe, Le Débat, n° 148, janvier-février 2008.

(4) Ibid.

Selon M[e] Alain Bensoussan, auditionné le 27 octobre 2010, alors que certains dénoncent les fausses informations qu'on trouve dans *Wikipédia*, cette dernière est devenue un dictionnaire mondial, un système d'intelligence collective qui ne comporte pas plus d'erreurs que les grandes encyclopédies traditionnelles. Ce système est devenu un standard universel d'information qui s'avère très résistant par rapport aux tentatives de manipulation.

La définition de *Wikipédia*, donnée par des collaborateurs locaux peut même s'avérer plus précise que celle des dictionnaires officiels. En outre, l'encyclopédie est à même d'offrir des mises à jour en permanence.

Quoi qu'il en soit, les wikipédiens sont les premiers à reconnaître que leur projet est complémentaire de celui des grandes encyclopédies faites par des experts.

Christian Vandendorpe, dans l'article précité, en conclut que « *tout comme l'ouvrage de Diderot et d'Alembert avait eu un impact considérable sur les mentalités du temps, il y a lieu de penser que Wikipédia contribuera de façon significative à modeler la culture virtuelle qui s'élabore en cette aube du XXI[e] siècle dans un monde globalisé.* »

2. Une démocratisation et un enrichissement des modes d'accès à la culture et de sa production

Avec le développement du numérique, ce ne sont pas seulement des possibilités inédites pour la diffusion des œuvres culturelles qui ont vu le jour, mais aussi de nouvelles pratiques culturelles, de nouvelles façons d'écouter de la musique, de regarder des films, de visiter des expositions ou des monuments et - bientôt sans doute – de lire un livre.

S'agissant de la musique, non seulement elle est consommée en plus grande quantité mais elle est à la fois mieux choisie et mieux adaptée aux goûts de chacun. Le bouche à oreille, autrefois limité à un cercle intime, s'étend aux communautés en ligne, c'est-à-dire à des réseaux immenses comme ceux qui se développent sur *MySpace.* Les modèles statistiques de prescription gagnent en finesse. Certains sites (comme *Itunes* avec le système *genius*) offrent à chaque internaute la possibilité de se déplacer dans un espace d'œuvres qu'il ne connaît pas encore mais qui correspondront à ses goûts et dont il peut écouter un extrait. Encore faut-il espérer que ces outils offrent véritablement à chacun un plus grand choix et l'accès à une plus grande diversité musicale et qu'ils ne conduisent pas au contraire à une homogénéisation des goûts musicaux et à un enfermement dans un univers musical donné.

Dans le domaine audiovisuel, l'avènement de la télévision numérique terrestre permet une augmentation considérable de l'offre culturelle grâce à la multiplication des chaînes et une amélioration incontestable de la qualité technique via la haute définition. Chacun peut en outre désormais accéder aux contenus diffusés par la radio et la télévision de façon délinéarisée (télévision de rattrapage, *podcasts* pour la radio).

Le numérique impose aux médias traditionnels, et en particulier au service public, une présence sur les nouveaux supports (Internet, réseaux sociaux, smartphones, tablettes numériques…).

C'est pourquoi l'un des objectifs majeurs de la réforme de l'organisation de la télévision publique opérée par la loi n° 2009-258 du 5 mars 2009 relative à la communication audiovisuelle et au nouveau service public de la télévision était, aux termes de l'exposé des motifs, de favoriser l'émergence d'un « média global », permettant de toucher tous les publics sur tous les supports. La loi sur le nouveau service public audiovisuel a ainsi élevé le développement numérique en priorité stratégique du groupe, et même en obligation.

Il est apparu qu'au-delà des ambitions affichées, il s'agissait d'une priorité qui ne faisait l'objet d'aucun financement identifié, ce qui se traduit par un retard important et difficilement justifiable du développement du service public audiovisuel sur les nouveaux supports. Lors de son audition par la commission des Affaires culturelles et de l'éducation le 12 juillet 2010, le nouveau président de France Télévisions, M. Rémy Pflimlin a reconnu ce retard. « *Vous l'aurez compris,* » a-t-il indiqué, « *le numérique doit devenir la colonne vertébrale de l'entreprise, qu'il s'agisse des contenus ou de la diffusion. France Télévisions doit rattraper son retard, notamment dans les échanges vidéo pratiqués sur les réseaux sociaux et dans la télévision de rattrapage : le portail de télévision de rattrapage de France Télévisions n'a été ouvert que le 2 juillet, alors que plus de dix millions de personnes consomment déjà régulièrement la télévision de rattrapage. Comment France Télévisions peut-elle devenir un acteur majeur et un laboratoire de l'innovation dans l'univers du numérique ? La responsabilité du numérique doit être confiée à un collaborateur, qui, à mes côtés, déterminera les objectifs en termes d'investissements, de développement d'offres et d'initiatives. Il faudra ensuite travailler sur l'« éditorialisation » des contenus afin que soit traitée, dès la conception des programmes, la question de leur diffusion sur l'ensemble des supports, chacun réclamant une forme différente. Nous devrons aussi relever deux autres défis : celui du temps réel, avec des sites événementiels à l'image du site dédié au Tour de France 2010 ; celui des réseaux sociaux et des sites de partage de vidéo, en donnant aux internautes la possibilité de « réagréger » des programmes, afin de se constituer leur propre offre – ce dernier point est crucial, s'agissant d'attirer les plus jeunes vers le service public.* »

Orientation n° 2 : garantir une présence forte du service public audiovisuel sur les nouveaux supports numériques

Au-delà du discours sur la priorité que constituerait le « média global » et de la nomination d'un responsable identifié, M. Bruno Patino, sur ce sujet**,** il est impératif que le nouveau contrat d'objectifs et de moyens du groupe France Télévisions, en cours de négociation, prévoie une stratégie crédible et ambitieuse de développement numérique accompagnée d'un financement qui soit à la hauteur des enjeux.

Il convient par ailleurs de s'assurer de la gratuité de l'accès aux contenus du service public sur ces nouveaux supports.

Enfin, la mission souhaite que soit engagée une politique volontariste de mise à disposition de certains programmes libres de droits dans des conditions permettant leur (ré)utilisation libre et gratuite, dans une démarche de co-création avec les internautes.

Le numérique a par ailleurs lui-même engendré une culture et des pratiques artistiques d'un genre nouveau, compte tenu des possibilités infinies de duplication et d'interactivité qu'il offre aux créateurs.

La créativité à l'œuvre dans les jeux vidéo a ainsi produit des référents et des codes marqueurs d'une « culture numérique » spécifique ou « cyberculture » qui est bien distincte de celle du cinéma ou de la télévision, et qui n'est plus aujourd'hui réservée à quelques « *geeks* » passionnés de nouvelles technologies.

De la même façon, les « arts numériques » qu'ils soient qualifiés de « dynamiques », « interactifs », « vectoriels » ou « multimédias » sont dépositaires de nouveaux courants dans les domaines de l'écriture, de l'image et du son, aux côtés des arts plus « classiques ».

Invité des rencontres *Regards sur le numérique* organisées par Microsoft, le 8 février dernier, M. Bernard Stiegler, philosophe et directeur de l'Institut de recherche et d'innovation du centre Pompidou, a analysé l'impact des nouvelles technologies sur le rapport des individus aux œuvres culturelles. « *Les gens âgés de plus de trente-cinq ans aujourd'hui ont pour la plupart été de gros consommateurs de flux. Nous avons entretenu un rapport consumériste aux œuvres culturelles. Un phénomène sans précédent, dans aucune autre société. Auparavant, les individus savaient lire des partitions musicales, on produisait de la musique à l'usine, à l'école, à l'église... Des compétences que les inventions comme la radio, puis la télé, ont rendues moins utiles, et qui ont progressivement disparu. Mais cet état de fait est aujourd'hui remis en cause par les principes collaboratifs et participatifs du Web* ». M. Bernard Stiegler estime que « *nous vivons actuellement un « second tournant machinique de la sensibilité », de la cognition et de l'intellect également : les* digital natives *ne veulent plus être de simples consommateurs, mais des producteurs, des agrégateurs de flux. Ils veulent redevenir des acteurs. C'est d'ailleurs grâce à cela que le monde de la culture est un terrain fertile en termes d'innovations numériques.* »

« *Aujourd'hui on peut monter des vidéos, les poster sur Internet… : c'est la réalisation du* Do It Yourself. *Il s'exerce ainsi un formidable transfert de compétences, grâce aux technologies, et ce qui était réservé à des professionnels, parce qu'extraordinairement complexe, devient accessible à tout le monde. On assiste en fait à une reconstruction de l'amateur dans le domaine culturel.* »

B. LE NUMÉRIQUE, PORTAIL D'ACCÈS À L'ENSEMBLE DU PATRIMOINE CULTUREL

Les technologies de l'information et de la communication offrent un moyen révolutionnaire d'accéder au patrimoine culturel existant et ce, à travers le monde entier. L'idée, jusque-là utopique, d'une bibliothèque universelle, accessible à tous devient, grâce aux technologies numériques, un objectif tout à fait réaliste dans un délai raisonnable. La perspective d'une numérisation systématique des œuvres laisse espérer la mise à disposition progressive sur le

réseau de l'ensemble du patrimoine de l'humanité. Les acteurs majeurs de cette entreprise sont à la fois les institutions publiques et *Google*. L'entreprise a développé avec des moyens et une efficacité spectaculaires un programme de numérisation pharaonique du patrimoine mondial au sens large, qui a pris de court toutes les institutions publiques.

1. L'ambition de *Google* : numériser le patrimoine mondial

Par-delà les nombreuses questions soulevées à juste titre par les modalités d'action de *Google* (absence de respect du droit d'auteur, de la vie privée et des données à caractère personnel, etc.) et dont il sera largement question dans la suite du présent rapport, on ne peut nier les apports de l'entreprise dans l'accès au savoir et à la culture.

La numérisation des contenus est en effet un enjeu majeur pour le moteur de recherche si celui-ci veut rester le maître incontournable de l'indexation. Sans les contenus, ses algorithmes tournent évidemment à vide. Pour faire tourner son moteur de recherche, *Google* doit avoir réponse à tout. C'est donc l'objectif que l'entreprise s'est fixé.

Le 14 décembre 2004, l'entreprise annonçait un projet de numérisation de 15 millions de livres en six ans

Environ 15 millions de livres ont ainsi été scannés depuis 2004 par *Google* Books, qui constitue aujourd'hui la plus grande bibliothèque du monde sur Internet. 30 bibliothèques, pour la plupart américaines, et sept européennes, ainsi que 35 000 maisons d'édition ont participé à ce projet. *Google* offre ainsi une nouvelle vie numérique à des millions d'ouvrages, oubliés sur les rayonnages des grandes bibliothèques et qui n'auraient probablement jamais été réédités. Le projet de numérisation des livres de *Google* mise avant tout sur la quantité, afin de tirer les bénéfices publicitaires liés au plus grand nombre possible de requêtes.

L'entreprise a souhaité, de surcroît, passer outre, au moins dans un premier temps, les obstacles légaux ou contractuels susceptibles de ralentir la réalisation de son plan. C'est ainsi qu'elle a cherché à imposer la confidentialité de ses accords avec les bibliothèques partenaires, exigée des clauses d'exclusivité sur les fichiers réalisés et leur indexation sur ses sites, ou numérisé des ouvrages sous droits, sans l'accord des auteurs ou des ayants droit, ce qui lui a valu une série de procès intentés par ces derniers.

En mars 2011, leurs craintes se sont certes un peu apaisées avec la décision très attendue rendue par la justice américaine (en délibération depuis un an), un jugement défavorable à *Google* et favorable aux auteurs comme aux éditeurs qui s'estimaient spoliés par la firme californienne.

Ces dix dernières années, *Google* a également lancé de nombreuses autres applications de recherche sur Internet, notamment *Google Images*, qui indexe plus

d'un milliard d'images, *Google Scholar*, moteur de recherche spécialisé dans les travaux académiques et scientifiques, *Google News Archive Search*, qui donne accès à des millions d'articles de presse, essentiellement en anglais, publiés depuis 200 ans, *Google Earth*, qui offre des images satellites de la terre, *Google Maps*, qui donne accès à des cartes et des plans de villes, *Google Street View*, service lancé en mai 2007 afin de compléter *Google Maps* et *Google Earth* et qui permet de naviguer virtuellement dans les rues de grandes villes ou encore *YouTube*, acquis en 2006 et qui, constituant le plus grand site d'hébergement de vidéos, a franchi en mai 2010 le cap des deux milliards de vidéos consultées quotidiennement. L'entreprise américaine numérise et indexe ainsi le monde qui nous entoure, notre patrimoine au sens large, à tel point que nous avons désormais besoin d'elle pour nous y retrouver.

En 2008, l'année où le magazine américain de photo-journalisme *Life* cessa de paraître, *Google* s'est vu confier par le groupe Time Warner la numérisation de près de dix millions de photos retraçant l'histoire du XX^{e} siècle et réalisées par les plus grands photographes tels que Richard Avedon ou Robert Capa. Les clichés numérisés, dont Time Warner a gardé les droits, sont accessibles à la fois sur son site Life.com et sur un serveur de *Google*.

En janvier 2009, *Google* a annoncé la réalisation d'une première mondiale : la mise en ligne de 14 chefs-d'œuvre du musée du Prado à Madrid, des tableaux de Vélasquez, Jérôme Bosch, Francisco Goya, Pierre Paul Rubens, Rembrandt et du Greco, numérisés en très haute définition, grâce à la technologie de *Google Earth*. Des centaines de clichés de chaque tableau, reproduisant chacun une petite partie de l'œuvre, ont été pris, ce qui permet d'obtenir un niveau de résolution tel qu'apparaissent des détails invisibles à l'œil nu.

C'est en utilisant la même technologie que *Google* a lancé, en février 2011, un nouveau site Internet (googleartproject.com) en collaboration avec dix-sept des plus grands musées au monde, dont le MOMA de New York, la *Tate Gallery* de Londres, le château de Versailles en France, l'*Alte Nationalgalerie* à Berlin, le *Rijksmuseum* d'Amsterdam ou encore le musée de l'Hermitage de Saint-Petersbourg. D'autres partenariats devraient être prochainement signés.

Utilisant la technologie de *Google Street View*, le site permet de visiter virtuellement les musées. Il est ainsi possible d'aller voir la disposition des œuvres au musée Van Gogh à Amsterdam d'un simple clic. De plus, pour chaque musée, une œuvre a été photographiée en très haute résolution (7 milliards de pixels), ce qui permet, là encore, de voir des détails pratiquement invisibles à l'œil nu. Outre l'œuvre en elle-même, *Google* propose une fiche explicative, des informations liées au musée, des liens renvoyant vers d'autres pages...

Ce projet a aussi pour ambition de redonner une image positive à *Google Street View* qui a été mise en cause dans de nombreux pays alors qu'elle avait « accidentellement » collecté des données privées. L'Art Project de *Google*

comporte de grands absents : le Louvre ainsi que les musées Guggenheim, par exemple.

Néanmoins, le projet est entièrement financé par *Google*. Après le programme de numérisation de livres, le moteur de recherche sur Internet s'attaque ainsi aux œuvres d'art. Le projet sera géré de Paris, où *Google* a annoncé l'ouverture d'un centre culturel.

Pour les musées, est-ce une chance ou un danger ? Ceux qui participent au projet sont pour l'instant enthousiastes : « *plus on a de visiteurs virtuels, plus on a de visiteurs réels : c'est ce qu'on constate depuis des années* », estime M. Denis Berthomier, administrateur du château de Versailles [(1)].

2. Une politique ambitieuse de numérisation de son patrimoine par l'État français

La mission estime que l'accessibilité du patrimoine à l'ère du numérique doit être appréhendée par les États comme une priorité pour l'avenir, dans la mesure où elle constitue un vecteur exceptionnel de la démocratisation de l'accès à la culture.

Nombreuses aujourd'hui sont les institutions publiques qui ont entamé la numérisation de leurs fonds à des fins de conservation et de transmission, en mettant à la portée de tous, en tout lieu et à tout moment, ce qui était jusqu'ici réservé à quelques-uns.

La France est l'un des rares pays à s'être donné les moyens de mener une politique publique ambitieuse de numérisation du patrimoine écrit. Les discussions entamées à l'été 2009 entre la Bibliothèque nationale de France (BNF) et *Google* pour la numérisation des livres auront servi de provocation et encouragé le Gouvernement à consacrer la somme de 750 millions d'euros, en provenance du « grand emprunt », à la numérisation des biens culturels. Seront les grands bénéficiaires de cette ressource : la BNF, le Centre national de la cinématographie (CNC), l'INA, les grands musées, l'Opéra de Paris ou encore la Cité de la musique.

Avec 13 millions de documents, la BNF est l'une des plus anciennes et des plus riches bibliothèques du monde. Environ 5 % de ses collections ont été numérisées à ce jour.

Comme l'a rappelé M. Bruno Racine, président de la BNF, lors de son audition du 1er décembre 2010, le premier programme de numérisation, lancé en 1995, avait pour objectif de procéder à une numérisation sélective portant sur les grands textes – les meilleurs morceaux des collections – ainsi que sur les documents conservés sur des supports particulièrement fragiles. Gallica, la bibliothèque numérique de la Bibliothèque nationale de France, lancée en 1997,

(1) La Tribune, *2 février 2011.*

avait ainsi comme ambition d'être la « bibliothèque virtuelle de l'honnête homme ».

Cependant, en 2005, en réponse à l'initiative de *Google*, qui avait fait part d'un projet pharaonique de numérisation de 15 millions de livres en six ans, Jean-Noël Jeanneney publie *Quand Google défie l'Europe*, essai dans lequel il plaide pour une réaction européenne et notamment française. Les annonces faites par *Google* ont conduit à un changement de paradigme, l'horizon de l'exhaustivité s'imposant depuis, même si, comme tout horizon, plus on s'en approche plus celui-ci s'éloigne.

Depuis 2007, une politique de numérisation de masse a ainsi été lancée, qui porte sur les documents tombés dans le domaine public, c'est-à-dire antérieurs au début du XX^{e} siècle. 12 millions de pages sont numérisées par an, soit 100 000 documents. On reste cependant loin de l'exhaustivité au regard des millions d'ouvrages présents dans les fonds.

Les documents numérisés deviennent accessibles gratuitement et à toute heure, y compris ceux qui, jusqu'alors, étaient réservés aux chercheurs accrédités. Tel a été le principe fondateur de la base *Gallica*, qui compte aujourd'hui 250 000 monographies et 800 000 numéros de revues, ce qui constitue le plus important ensemble de documents francophones du monde, plus riche que *Google*. *Gallica* donne accès, en outre, à 30 000 ouvrages provenant d'autres bibliothèques et la prochaine campagne de numérisation portera pour deux tiers sur le fonds de la BNF et pour un tiers sur des fonds extérieurs.

En mars 2008, toujours pour répondre à *Google*, a été lancé un projet d'intégration dans *Gallica* d'œuvres sous droits, en partenariat entre la BNF, la direction du livre et de la lecture, le Centre national du livre et le Syndicat national de l'édition. Ces documents sont indexés sur *Gallica* ; mais pour accéder à leur contenu l'internaute est redirigé vers la plateforme commerciale de l'éditeur.

Par la richesse et la diversité des collections qu'elle propose en ligne et par les technologies qu'elle met en œuvre, *Gallica* constitue une des premières bibliothèques numériques au monde.

Cependant, dans un rapport récent du Conseil d'analyse de la société, *La révolution du livre numérique,* M. Marc Tessier observe que les fonds qui figurent sur Gallica sont difficilement accessibles à moins que l'internaute soit suffisamment averti pour se rendre directement sur Gallica. « *C'est pourquoi il faudra veiller à ne plus numériser pour numériser mais aussi pour assurer un accès facile à ces fonds, ce qui implique de réfléchir très en amont sur les moyens à mettre en œuvre pour qu'ils puissent être plus « repérables », selon une autre expression consacrée (référencement, indexation, citations dans les blogs ou des sites, etc.), ce que Gallica a entrepris de faire… mais avec retard.* »

La BNF a finalement fait jouer la concurrence en faisant appel, non pas à *Google*, mais à Bing, le moteur de recherche de Microsoft, chargé d'améliorer sa

visibilité sur Internet et à un moteur de recherche français, Exalead, filiale de Dassault Systèmes.

S'agissant des actions entreprises par la BNF pour faire connaître son fonds à un large public, M. Bruno Racine a expliqué que le nouveau moteur de recherche en cours de mise en place traduisait la volonté d'aller au-devant des préoccupations des internautes. La BNF publie, par ailleurs, sur son site une lettre d'information et un blog ; elle indique les documents les plus consultés et est également présente sur les réseaux sociaux. Tous les efforts sont faits pour proposer un site Internet vivant, enrichi de plus de 2 000 documents nouveaux par semaine ; la consultation des documents de presse connaît par exemple un grand succès.

La BNF a en outre développé un réseau tourné vers le public scolaire, en particulier les enseignants, et participe à de nombreux projets pédagogiques utilisant de plus en plus les documents accessibles sur *Gallica*. A été ainsi relancée la série des classiques de *Gallica* et une histoire du livre sera bientôt mise en ligne à destination d'un jeune public.

Cependant, M. Bruno Racine, président de la Bibliothèque nationale de France, a également attiré l'attention de la mission sur le fait que préservation du patrimoine ne portait pas seulement sur les documents anciens mais prenait en compte tout ce qui naissait aujourd'hui sur des supports issus des nouvelles technologies. **Or, il est à regretter que le décret devant préciser les dispositions du code du patrimoine, adoptées en 2006, dans le cadre de la loi n° 2006-961 relative aux droits d'auteur et aux droits voisins dans la société de l'information, par lesquelles la BNF, et accessoirement l'Institut national de l'audiovisuel (INA), se sont vus confier la mission du dépôt légal des documents créés sur support numérique ne soit pas encore paru**. En effet, le retard que connaît la publication de ce texte laisse jusqu'à présent en suspens les modalités de sélection, d'archivage et de communication de ce type de document. **La mission souhaite qu'il soit enfin mis un terme à ce vide juridique.**

La numérisation porte aussi sur le patrimoine monumental français. Le programme de numérisation « 3D Monuments » permet, outre sa conservation par la prise d'empreinte numérique, une valorisation au bénéfice du grand public, en donnant à voir, à revoir et donc à comprendre par le plus grand nombre l'objet étudié sur des supports variés allant de l'image fixe à l'image animée diffusée sur cédérom ou sur des dispositifs muséographiques immersifs (1) ou encore en ligne sur le réseau Internet. Ce programme offre par exemple une visite virtuelle du Petit Trianon : les meubles qui ont disparu ou qui se trouvent à l'étranger sont reconstitués, ceux qui ont été transformés sont restitués dans leur état d'origine. L'intérêt culturel et pédagogique de cette modélisation est incontestable et l'on attend avec impatience le « Grand Versailles numérique ».

(1) Dispositifs de visualisation utilisés pour « immerger » le visiteur dans une scène en 3D.

L'un des premiers musées présent sur Internet, dès 1995, le Louvre propose un site vivant et interactif. Dans la perspective de sa refonte prévue pour la fin de l'été 2011, une plate-forme communautaire expérimentale dédiée à l'histoire de l'art, Communauté Louvre, a été mise en place. L'idée est de faire participer activement à l'alimentation du site : partage des photos et des vidéos prises dans le musée, rédaction d'articles sur des œuvres ou des articles, dialogues entre amateurs… S'inspirant d'une initiative du *Brooklyn Museum*, le Louvre propose aussi aux internautes de contribuer à l'indexation des œuvres en leur associant des mots clés (thème, émotion, couleur…). Cette indexation spontanée doit compléter l'indexation scientifique des conservateurs.

S'agissant des archives audiovisuelles, elles ont bénéficié d'un plan de sauvegarde et de numérisation (PSN), engagé dès 1999 par l'Institut national de l'audiovisuel (INA). Auditionné par la mission le 1er décembre 2010, M. Mathieu Gallet, président-directeur général de l'institut, a souligné l'évolution de l'exercice de la mission que lui confie l'article 49 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, à savoir « *conserver et mettre en valeur le patrimoine audiovisuel national* ». En effet, les fonds de l'INA étaient auparavant cachés, réservés à des professionnels, réalisateurs, producteurs, chaînes de télévision, qui devaient venir chercher, parmi les centaines de milliers de cassettes que conservait l'INA, les images dont ils avaient besoin. La révolution d'Internet a permis d'offrir au grand public un accès à ces fonds.

En ce qui concerne la manière de s'adresser au grand public, M. Mathieu Gallet a rappelé que l'on pouvait avoir deux conceptions. La première conception, celle des grands opérateurs mondiaux, tels que *Google*, *YouTube* ou *Facebook*, consiste à mettre à la disposition du public des milliards d'images « en vrac ». La conception de l'INA est différente de celle des sites hébergeurs agrégeant des contenus. En tant qu'établissement public, et compte tenu de la spécificité de son fonds qui est de nature patrimoniale et participe ainsi à la mémoire du pays, l'INA a un rôle d'éditorialisation de ce fonds : il doit lui donner du sens, le penser par rapport aux grands thèmes de société, à l'histoire, la culture, le divertissement.

L'État consacre chaque année un budget très important pour aider l'INA. En dix ans ce sont 100 millions d'euros qui ont été affectés au plan de numérisation, et 51 millions d'euros supplémentaires le seront dans les cinq ans à venir. L'INA a numérisé aujourd'hui un peu plus de 70 % de son fonds. À la fin du contrat d'objectifs et de moyens (COM) actuel, fin 2014, l'INA devrait avoir numérisé environ 88 % de ce fonds.

En réponse à l'observation du CSA sur le projet de COM, qui estime que la mise à la disposition du fonds au grand public est insuffisante, M. Mathieu Gallet a rappelé que l'objectif de l'INA, d'ici à fin 2014, était de passer de 26 000 heures de documents accessibles sur le site ina.fr, objectif dépassé en 2007, à 40 000 heures. Cela nécessite un travail important car, encore une fois, il ne s'agit pas simplement de mettre le fond de 1 600 000 heures en ligne « en vrac » mais bien de penser l'offre et de l'éditorialiser.

Cependant, M. Mathieu Gallet a également souligné la nécessité pour l'INA « d'essaimer » au-delà de son site Internet, afin de pouvoir toucher le jeune public, là où il se trouve, c'est-à-dire sur les plateformes telles que *YouTube, Dailymotion ou Facebook*. L'institut a d'ailleurs signé, en novembre 2010, un accord avec *Dailymotion* qui lui permet de mettre en ligne 50 000 vidéos déjà accessibles sur ina.fr mais auxquelles le public, qui ignore l'existence du site, n'accède pas. *Dailymotion* les met en ligne dans un espace clairement identifié « ina » et selon des thématiques répertoriées, qui sont celles que le grand public recherche, c'est-à-dire l'actualité, le divertissement, etc. Le « Journal du jour de votre naissance » a ainsi été mis en avant par *Dailymotion.* Cette fonctionnalité existait sur le site ina.fr mais n'attirait que 1 700 000 visiteurs par mois contre près de 10 000 000 sur *Dailymotion*.

S'agissant du patrimoine cinématographique français, le 10 mai 2011, a été signé à Cannes un accord-cadre présenté comme « historique » pour le financement de la numérisation des œuvres cinématographiques par les ministres de la Culture et de l'Industrie et les principales sociétés propriétaires de catalogues (EuropaCorp, Gaumont, Pathé, SND, StudioCanal, TF1 Droits audiovisuels...). À terme 10 000 films, 10 millions de bobines devraient être numérisés. Les longs métrages postérieurs à 1929, les films de Jean Cocteau, Julien Duvivier, René Clair et Alain Resnais, comptent parmi les 2 500 premières œuvres concernées par ce plan de numérisation.

Piloté par le Centre national du cinéma et de l'image animée (CNC), ce programme de numérisation sera doté d'un budget de 100 millions d'euros et bénéficiera de crédits du grand emprunt. La France, qui avait déjà investi 125 millions d'euros pour la numérisation des salles de cinéma, est aujourd'hui l'un des premiers pays à mettre en place un dispositif complet de financement de la numérisation et de la restauration des œuvres du patrimoine.

3. Les projets de numérisation lancés par d'autres institutions publiques en Europe et à l'étranger

En novembre 2008, la Commission européenne a lancé un projet de point d'accès à des œuvres du patrimoine, associant de nombreuses institutions des 27 pays de l'Union européenne et baptisé Europeana.

M. Bruno Racine a précisé que le site *Europeana* n'avait pas de fonds documentaire propre mais était un portail donnant accès à différentes bibliothèques, centres d'archives et fonds audiovisuels. Si ce site, qui présente la particularité d'être multilingue, permet l'accès à plus de 13 millions de documents de toute nature (livres, tableaux, œuvres musicales, photographies, films, cartes, manuscrits, partitions…), il ne bénéficie malheureusement pas d'une fréquentation élevée et son périmètre d'action est mal défini. Selon M. Bruno Racine, son succès dépendra du développement des outils d'organisation de la masse d'informations proposée mais l'avenir d'*Europeana* apparaît pour l'heure incertain, comme en atteste la diminution très importante des accès à *Gallica via* ce site.

Le président de la BNF regrette que la Commission européenne ait privilégié une vision très large du champ d'*Europeana*, non limitée au domaine du livre, mais étendue à la totalité du patrimoine culturel, une ambition, qui pour se concrétiser, aurait nécessité des moyens financiers considérables. Or, la Commission européenne n'entend pas financer cette numérisation puisqu'elle estime être principalement du ressort des États, lesquels, pour la plupart, n'en font pas une priorité, encore moins depuis la crise financière. Dans un rapport récent du Conseil d'analyse de la société consacré à la révolution du livre numérique, M. Bruno Racine en conclut que « *si la bibliothèque numérique européenne au sens où nous l'entendions au départ a bien pris forme, c'est chez* Google *! Un exemple : en 2010, Goethe en allemand restait introuvable sur Europeana, qui ne donne accès qu'à sa traduction… en français ou en hongrois. En revanche, le texte original est depuis longtemps accessible sur* Google Livres. »

La Commission européenne a, par ailleurs, financé un projet à dimension européenne baptisé *Europeana Regia*, qui a procédé à la numérisation complète d'un certain nombre de bibliothèques royales datant du Moyen Âge et de la Renaissance dont les inventaires sont connus, comme la bibliothèque des rois aragonais de Naples et la bibliothèque de Charles V au Louvre. Selon M. Bruno Racine, de tels projets ciblés sont la voie d'avenir au plan européen, plutôt que l'accumulation de ressources de qualité très inégale. Globalement, la conception des projets à l'échelle européenne manque de clarté. L'intérêt, pour toutes les bibliothèques, serait par conséquent de disposer d'une structure de coordination européenne sur la base de coordinateurs nationaux.

En Europe, la numérisation du patrimoine fait l'objet de nombreuses autres réalisations qui viennent enrichir les grands portails culturels nationaux comme l'allemand BAM (bibliothèques, archives, musées), l'italien Culturaltalia ou le français Culture.fr/Collections. Des réseaux se créent, fédérant des initiatives nationales, afin d'offrir un accès unique aux archives.

Ainsi, le projet de portail *European Film Gateway* (EFG), destiné aux cinémathèques européennes, a-t-il été lancé en septembre 2008 et regroupe 20 partenaires de 14 pays.

Le projet *GAMA* (*Gateway to Archives of Media Art*), lancé en décembre 2007, est consacré aux arts multimédias en Europe grâce à l'engagement de 19 institutions de 12 pays.

La diversité des travaux entrepris démontre la volonté d'étendre ce processus de numérisation au patrimoine qualifié d'immatériel, incluant les arts du spectacle, les traditions et expressions orales, les pratiques sociales. En témoignent les projets en cours de réalisation en Europe concernant, par exemple, les archives sur la généalogie ou sur l'histoire locale, les corpus oraux (enregistrements sonores) offrant une connaissance des langues dans toute leur variété, les archives audiovisuelles consacrées aux spectacles et musiques du monde ou encore à l'activité des orchestres en France.

Un autre grand chantier numérique a été inauguré en avril 2009 : la Bibliothèque numérique mondiale (BNM) de l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), qui se construit autour du parti pris d'une sélection étroite des œuvres du patrimoine mondial. La BNM est née d'un partenariat d'une trentaine de pays auxquels se sont associées des fondations et des entreprises privées, au nombre desquelles figurent Microsoft et *Google*. En décembre 2009, l'UNESCO a choisi de confier à *Google* la mise en ligne des sites naturels ou architecturaux inscrits au patrimoine mondial. Sur les 890 sites ainsi recensés, 19 ont été sélectionnés pour être offerts en consultation aux internautes du monde entier, dont le château de Versailles en France, le centre historique de Prague et la vieille ville espagnole de Caceres. D'autres documents seront ultérieurement numérisés par *Google* afin d'être mis en ligne, des cartes, des textes, des vidéos portant sur les réserves de biosphère ou encore les langues menacées de disparaître.

C. L'UNIVERS NUMÉRIQUE, QUELS RISQUES POUR LA CULTURE

1. Le débat sur le rôle des acteurs privés dans la numérisation du patrimoine écrit

Malgré l'enthousiasme que suscite, quant au principe, la perspective d'une numérisation et d'une mise à disposition massive des œuvres du patrimoine écrit sur Internet, les conditions dans lesquelles cette idée prend corps soulèvent de nombreuses interrogations, touchant essentiellement au rôle que peuvent jouer les acteurs privés, au premier rang desquels, *Google*.

L'annonce par *Google*, le 14 décembre 2004, d'un projet de numérisation de 15 millions de livres en six ans a suscité la crainte d'une mainmise d'un opérateur privé en position dominante sur la diffusion du patrimoine écrit. De nombreux observateurs ont estimé qu'un seul acteur privé ne pouvait assurément pas assumer la responsabilité de structurer et organiser la majeure partie des savoirs recopiés sur le Web. Quoi qu'il en soit, l'entreprise de Mountain View a pris de court toutes les institutions culturelles d'État. Par manque de réactivité, de moyens et de coordination, les projets européens ou internationaux se sont déployés trop lentement.

Face à cette situation, trois types de stratégies, s'agissant de la numérisation du patrimoine, se sont opposés en France.

À l'été 2009, l'annonce de discussions entre la BNF et *Google* pour la numérisation et la mise en ligne de son fonds a provoqué une intense polémique. On apprenait également que la bibliothèque municipale de Lyon, suivie depuis par d'autres bibliothèques publiques européennes, avait conclu un accord avec *Google* lui concédant vingt-cinq ans d'exclusivité sur l'exploitation numérique de ses fichiers.

S'agissant de la numérisation des fonds des bibliothèques, dans un avis rendu public le 14 décembre 2010 sur le fonctionnement de la concurrence dans le secteur de la publicité en ligne, l'Autorité française de la concurrence considère que la clause d'exclusivité de 25 ans, avec interdiction de faire numériser le fonds par une autre entreprise durant toute cette période inscrite dans l'accord passé entre la Bibliothèque de Lyon et le moteur de recherche *Google* était « *exagérée au regard du rythme de changement du secteur* » et qu'« *il ne peut être admis de priver un moteur de recherche de la possibilité de répliquer à* Google *en investissant par ses propres moyens dans la numérisation* ». Dans une lettre adressée à l'Autorité de la concurrence au cours de l'instruction, *Google* a précisé que ces clauses, qui n'ont pas été introduites à sa demande, ne seront pas mises en œuvre.

Dans le cadre des négociations entamées en 2009 avec *Google*, M. Bruno Racine, président de la Bibliothèque nationale de France, avait proposé d'explorer la possibilité d'un « partenariat exigeant » : il souhaitait confier à la firme américaine, pourvu qu'elle accepte de réduire la durée de l'exclusivité des droits d'indexation et de propriété qu'elle se réserve sur les fichiers, la numérisation d'ouvrages qu'elle se déclarait prête à réaliser rapidement, pour pouvoir réaffecter le budget ainsi économisé sur des projets que la BNF était seule à pouvoir piloter : numérisation de documents rares, amélioration des moteurs de recherche et des métadonnées, entretien et modernisation des fichiers, etc. L'idée était également d'assurer un surcroît de visibilité à notre patrimoine *via* le moteur de recherche le plus consulté. Le tollé médiatique provoqué en France par l'ouverture de ce dialogue avec *Google* a conduit à l'interruption des discussions.

M. Jean-Noël Jeanneney, président de la BNF de 2002 à 2007, estime, quant à lui, que le principe de l'inaliénabilité de notre patrimoine s'oppose radicalement à ce que les pouvoirs publics délèguent leur responsabilité en matière de numérisation de l'écrit et partagent la propriété des fichiers avec d'autres acteurs. Il plaide donc pour une action volontariste sur fonds publics, en concertation avec nos partenaires européens, et pour le développement d'un moteur européen, concurrent de *Google*.

Il lui semble de surcroît crucial de proposer à l'internaute des réponses organisées selon des critères culturels élaborés par des experts plutôt qu'une offre « en vrac », hiérarchisée en fonction des seuls liens établis spontanément par les internautes, comme c'est largement le cas dans les référencements réalisés par *Google*. Il considère, en effet, que c'est la seule manière de remplir correctement la fonction éducative d'une bibliothèque, particulièrement auprès des publics peu cultivés.

Ce point de vue n'est pas partagé par M. Bruno Racine, qui juge la présentation « en vrac » plus intuitive et plus souple d'utilisation, quitte à recourir à d'autres outils d'exploration lorsque l'on entreprend une recherche plus ciblée.

M. Marc Tessier s'est efforcé, dans le rapport qui lui avait été demandé sur ce thème en 2010, de concilier les positions de Bruno Racine avec les principes défendus par M. Jean-Noël Jeanneney. Il estime qu'il peut être dangereux de laisser un unique acteur privé maître de la numérisation. Il est selon lui impossible de s'assurer que les fichiers seront tous de qualité identique. En outre, les accords avec *Google* impliquant en général des clauses d'exclusivité d'exploitation commerciale, le référencement sur Internet des ouvrages numérisés dépendrait donc de la volonté de la société américaine.

M. Marc Tessier a donc proposé un système d'échange de fichiers entre *Google* et les bibliothèques publiques sans droit d'exclusivité : la bibliothèque apporterait à *Google* les collections qu'elle a elle-même numérisées, en contrepartie de quoi le moteur de recherche serait chargé de référencer les fichiers correspondants afin que l'on puisse les trouver facilement et *Google* verserait sur le site de la bibliothèque des fichiers numérisés par ses soins. Cette contribution a été saluée par toutes les parties, qui y voient un bon point de départ pour relancer la discussion.

Aujourd'hui, comme il a été indiqué précédemment, les crédits du grand emprunt dédiés à la numérisation du patrimoine écrit ont largement modifié la donne et la BNF a finalement fait jouer la concurrence en faisant appel, non pas à *Google*, mais à *Bing*, le moteur de recherche de *Microsoft*, chargé d'améliorer sa visibilité sur Internet ainsi qu'à un moteur de recherche français, Exalead, filiale de Dassault Systèmes.

La France, qui a pris une longueur d'avance sur ses partenaires européens en matière de numérisation de son patrimoine, a un rôle essentiel à jouer en Europe. En novembre 2009, les ministres de la Culture de l'Union européenne se sont ainsi entendus sur l'idée émise par la France de créer un « comité des sages », chargé de définir les modalités de futures collaborations entre le secteur public et le secteur privé pour financer la numérisation du patrimoine culturel.

En avril 2010, ce comité a remis un rapport se concluant par d'importantes recommandations mais insistant surtout sur la question essentielle du financement.

La France a choisi de mener un programme ambitieux de numérisation de son patrimoine. L'annonce d'une enveloppe spécifique allouée à la numérisation du patrimoine culturel dans le cadre du grand emprunt permet d'ailleurs de retrouver de réelles marges de manœuvre pour mener une politique autonome et bénéficier d'une situation plus équilibrée lorsqu'il s'agit de négocier avec des partenaires privés.

Cependant, d'autres pays européens ont prévu des budgets plus restreints. C'est pourquoi le rapport du comité de sages préconise une augmentation considérable par les États membres des fonds consacrés à la numérisation du patrimoine. Les fonds nécessaires à la construction de 100 km de routes pourraient

financer la numérisation de 16 % de tous les livres disponibles dans les bibliothèques de l'Union européenne, ou la numérisation du contenu audio que détient l'ensemble des institutions culturelles des États membres.

Indiquant que près de 100 milliards d'euros seront nécessaires pour rendre la totalité du patrimoine européen disponible en ligne, le rapport préconise l'encouragement de partenariats public-privé sous certaines conditions.

Les accords passés devront être transparents, non exclusifs et équitables pour tous les partenaires et permettre à tous un accès transfrontalier au matériel numérique.

Le droit à une utilisation préférentielle des œuvres numérisées octroyé, le cas échéant, à un partenaire privé ne pourra excéder une durée de sept ans.

Le rapport réaffirme le rôle central du portail Europeana qui devrait devenir la référence première pour le patrimoine culturel européen en ligne. Les États membres devront garantir que toutes les œuvres numérisées grâce à des fonds publics seront accessibles sur son site. Tous les chefs-d'œuvre du domaine public devraient être en ligne sur Europeana d'ici à 2016.

En outre, les œuvres épuisées protégées par le droit d'auteur doivent être mises en ligne par leurs ayants droit et à défaut, par les institutions culturelles, les ayants droit étant rémunérés en conséquence.

S'agissant des œuvres orphelines, le rapport préconise l'adoption au plus vite d'un instrument juridique européen. Afin d'éviter à l'avenir que les ayants droit ne soient pas identifiables, le rapport préconise que l'enregistrement de l'auteur d'une œuvre devienne une condition nécessaire pour que ce dernier puisse faire valoir ses droits. Une modification de la Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886 sur ce point doit être discutée afin de l'adapter aux exigences de l'ère numérique.

Les recommandations du rapport du Comité des sages seront prises en compte par la Commission européenne dans le cadre de sa « stratégie numérique pour l'Europe » dont le but est d'accompagner les institutions culturelles dans leur transition numérique.

Selon la commissaire européenne chargée des nouvelles technologies, Mme Viviane Reding, l'Europe doit également établir sa propre législation en matière de propriété intellectuelle en définissant des normes pour la numérisation protégeant les droits des auteurs et assurant leur rémunération. Des systèmes de licences et de rémunérations supranationaux devront être établis afin de faciliter l'accès aux contenus numérisés les plus récents, entravé jusqu'ici par les législations nationales sur le droit d'auteur.

L'ÉPINEUSE QUESTION DE LA NUMÉRISATION DES ŒUVRES ORPHELINES

Comme M. Bruno Racine l'avait indiqué à la mission lors de son audition du 1er décembre 2010, en posant comme césure temporelle les documents antérieurs au XXe siècle, le fonds numérisé comporte un « trou noir » puisqu'il n'inclut pas les ouvrages du XXe siècle encore sous droits mais indisponibles dans le commerce et sans ayant droit identifié.

En cette matière, la politique de *Google* a consisté à numériser indifféremment les œuvres sous droits et libres de droits en s'efforçant ensuite de négocier, à partir d'une position de force, des compromis avec les plaignants, en cas de procès.

En novembre 2010, Hachette a signé un protocole d'accord avec *Google*, autorisant ce dernier à numériser et à exploiter commercialement 40 000 à 50 000 ouvrages épuisés et partant, indisponibles à la vente, dont les droits sont administrés par le premier éditeur français. Cet accord avait suscité des remous dans le monde de l'édition car le Syndicat national de l'édition, dont Hachette est membre, était en procès contre *Google* à la suite à la numérisation par la firme californienne d'ouvrages sous droits, sans l'accord de leur maison de publication (Le Seuil–La Martinière). Cependant, contrairement à l'accord signé par *Google* en 2008 avec la Bibliothèque municipale de Lyon, le protocole signé avec Hachette prévoit la remise de chaque fichier numérisé à la BNF, qui pourra donc assurer ses missions de conservation et de mise à disposition du patrimoine culturel écrit. Les auteurs et les libraires ont vu dans cet accord un renforcement de la domination du géant *Google* sur le marché du livre numérique. Le Syndicat de la librairie française (SLF) a manifesté son inquiétude au regard d'une plus grande dépendance que cette nouvelle *entente* leur impose vis-à-vis du géant américain qui devient ainsi « *pour les librairies, à la fois l'un de leurs concurrents majeurs dans la diffusion commerciale des œuvres, l'un de leurs fournisseurs potentiels de contenus et de services et le principal portail d'accès au public vers leurs sites Internet* ».

Quant au ministre de la Culture et de la communication, M. Frédéric Mitterrand, engagé sur la question de la numérisation des œuvres aux côtés des professionnels de l'édition, il a regretté le manque de concertation, la décision du groupe Hachette brisant quelque peu le consensus établi entre les éditeurs français pour faire face au géant américain.

En réponse à cette initiative isolée, un accord prévoyant la numérisation sur cinq ans, grâce à une subvention accordée dans le cadre du grand emprunt, de 500 000 ouvrages du XXe siècle, sous droits mais épuisés, a été signé le 1er février 2011 entre le ministère de la Culture et de la communication, la BNF, le Syndicat national de l'édition (SNE), la Société des gens de lettres (SGDL) et le Commissariat général à l'investissement du gouvernement. Ces livres seront numérisés par la BNF, qui possède un ou plusieurs exemplaires de chaque ouvrage publié en vertu du dépôt légal. Ils seront ensuite référencés sur Gallica, et il sera possible d'en feuilleter quelques pages en ligne. Les internautes qui souhaiteront se les procurer seront dirigés vers des sites marchands grâce à des liens proposés par Gallica. Ainsi, des milliers de livres indisponibles en librairie pourront-ils retrouver un public et sortir de l'oubli.

Afin de garantir les droits des auteurs et des éditeurs, ceux-ci seront représentés de façon paritaire au sein d'une société de gestion collective chargée de l'exploitation des titres numérisés. Cependant, le code de la propriété intellectuelle prévoit que l'exploitation numérique de ce type d'ouvrages ne peut se faire sans la signature d'un avenant par les ayants droit concernés. Or, retrouver les ayants droit d'un demi-million de livres écrits au siècle dernier est matériellement impossible. Il est donc nécessaire d'amender la loi pour permettre la mise en œuvre de ce programme de numérisation.

Le coût de numérisation de ces 500 000 livres est pour l'instant estimé à 50 millions d'euros, mais une étude de faisabilité va être réalisée pour « préciser les modèles économiques et financiers », a déclaré le ministre de la Culture Frédéric Mitterrand, dans son discours prononcé à l'occasion de la signature de l'accord.

La mission se félicite de cette démarche de numérisation d'ouvrages par une institution publique nationale, qui témoigne de la volonté des autorités françaises de se réapproprier le processus de dématérialisation des contenus culturels écrits du pays en réponse à *Google*.

S'agissant des œuvres sous droit, face à de nouvelles formes de concurrence (*Amazon*, *Google*…) et pour éviter le piratage massif qui a touché l'industrie musicale, les éditeurs et les libraires tentent de s'organiser, même si la diversité

des entreprises et la multiplicité des intérêts rendent difficile le ralliement à une ligne commune. En dépit du souhait maintes fois exprimé de voir naître une plate-forme unique pour l'offre légale de livres numériques en France, on en recense aujourd'hui trente-et-une, dont quatre principales. Les distributeurs et les libraires se plaignent de la difficulté pour eux et pour les lecteurs d'accéder, dans ces conditions, aux ouvrages numérisés par les éditeurs (environ 60 000 pour 650 000 titres en format papier).

Afin de pallier les problèmes induits par cet éclatement des structures et des métiers qui touchent directement ou indirectement à la « chaîne du livre », Mme Christine Albanel, alors ministre de la Culture, a proposé dans un rapport d'avril 2010, la création d'un groupement d'intérêt économique (GIE) du livre français qui rassemblerait en son sein partenaires publics et privés, avec tous les acteurs du monde du livre. Une telle structure aurait vocation à porter une politique commune de numérisation, de diffusion et de partenariat avec les grands moteurs de recherche. Elle devrait également favoriser la constitution d'un portail interprofessionnel qui permettrait de faire le lien entre les plates-formes des éditeurs et des libraires. Le progrès serait indéniable. Reste qu'il serait imprudent de ne pas tenir compte du déséquilibre inévitable entre la capacité de réactivité d'une puissante firme indépendante et les lourdeurs qu'engendrent nécessairement les conflits d'intérêts dans les structures fédératives.

Parmi les mesures récemment adoptées pour favoriser le développement d'un marché du livre numérique, on peut se féliciter de l'adoption de la n° 2011-590 du 26 mai 2011 relative au prix du livre numérique qui étend la loi n° 81-766 du 10 août 1981, dite « loi Lang », ayant instauré le système du prix unique du livre « papier » : chaque livre a un prix fixé par l'éditeur ou par l'importateur, ce prix s'imposant à tous les détaillants. Le prix unique du livre numérique s'appliquera désormais en France, mais aussi aux plates-formes établies à l'étranger lorsque les acheteurs sont situés en France. Cette clause d'extraterritorialité étant contestée par la Commission européenne, la France va désormais devoir défendre son texte auprès des institutions européennes.

On voit combien les questions soulevées par la numérisation de l'écrit sont nombreuses et délicates à résoudre. *Google* a certes pris une avance substantielle en Europe dans la numérisation du patrimoine écrit. L'entreprise a su négocier au cas par cas et signer des accords dans tous les pays importants de l'Union.

Selon M. Bruno Racine, dans le rapport précisé du Conseil d'analyse économique, il est regrettable que l'Europe n'ait pas réfléchi plus tôt aux conditions d'un partenariat équilibré avec *Google* sans monopole, ni aux moyens qu'il aurait fallu engager pour lancer une alternative crédible. Les accords conclus avec les bibliothèques européennes auraient pu être plus favorables et il y aurait aujourd'hui des millions de livres sur Europeana. Unie, l'Europe aurait pu fixer un cadre inattaquable pour éviter le monopole et faire respecter le droit d'auteur.

La mission estime qu'il n'est pas trop tard pour une action collective européenne. L'Europe doit en effet pouvoir se présenter unie dans ses exigences, notamment sur le respect du droit d'auteur et les contreparties à accorder aux partenaires privés en général.

Orientation n° 3 : établir un cadre favorable à la numérisation du patrimoine, vecteur exceptionnel de démocratisation de l'accès à la culture

La mission estime que la numérisation du patrimoine doit être considérée par les États comme une priorité pour l'avenir. Elle préconise par conséquent :

– que notre pays poursuive les efforts financiers en faveur de la numérisation du patrimoine ;

– que la France, qui a pris une longueur d'avance sur ses partenaires européens en la matière, incite ses partenaires européens à amplifier leurs efforts et à se doter d'un cadre commun définissant les modalités d'un partenariat équilibré avec les partenaires privés, tels que *Google*, pour faire respecter le droit d'auteur et éviter que ces derniers ne soient en position de dicter leurs conditions ;

– que l'on veille à ne pas « numériser pour numériser » mais que l'accent soit mis sur les moyens de faciliter et de développer l'accès par le plus grand nombre aux fonds numérisés, quels qu'ils soient (fonds de l'INA, de la BNF…), ce qui implique de réfléchir très en amont sur les moyens à mettre en œuvre pour qu'ils puissent être plus « repérables » (référencement, indexation des contenus, citations dans les blogs, les réseaux sociaux ou les sites les plus consultés, etc.) :

– que soit rapidement publié le décret qui doit préciser les dispositions du code du patrimoine, adoptées en 2006, dans le cadre de la loi n° 2006-961 relative aux droits d'auteur et aux droits voisins dans la société de l'information, par lesquelles la BNF, et accessoirement l'Institut national de l'audiovisuel (INA), se sont vus confier la mission du dépôt légal des documents créés sur support numérique.

2. La copie numérique : une espérance de vie limitée

Si certains s'inquiètent de l'absence d'un droit à l'oubli sur Internet, d'autres redoutent que le numérique ne nous impose un oubli général à très court terme… Nos données numériques sont en effet programmées pour disparaître. Une étude publiée par l'Académie des sciences et l'Académie des technologies en mars 2010 confirme ce que nous redoutons le plus : l'enregistrement de nos données, textes, photos, vidéos, est périssable.

Si la numérisation des contenus en facilite la production, la diffusion et le stockage, elle n'en assure pas pour autant la conservation. L'espérance de vie des supports numériques est en effet très courte, de 5 à 10 ans. Intitulée « Longévité de l'information numérique. Les données que nous voulons garder vont-elles s'effacer ? », une étude menée par un groupe de travail commun à l'Académie des sciences et à l'Académie des technologies nous alerte sur la possibilité d'un *disk crash* à grande échelle et donne quelques pistes pour parer au plus pressé. Pour

M. Jean-Charles Hourcade, l'un des auteurs de l'étude, « *Il n'existe pas de modèle économique pour concevoir des supports fiables* », les consommateurs n'ayant pas encore pris conscience de la gravité du problème de la conservation des données numériques.

Le rapport conclut par quatre recommandations, afin de sauvegarder les données numérisées, que la mission reprend à son compte.

Orientation n° 4 : assurer la sauvegarde des données numérisées

– débloquer les études sur le sujet. Engager rapidement une étude réellement scientifique des phénomènes de vieillissement des supports, notamment des supports optiques, visant à dégager des recommandations fiables en matière de standardisation de formats de supports d'archivage longue durée. Lancer rapidement un appel à projets ambitieux visant à remplacer la technologie d'enregistrement optique actuelle (CDR et DVDR), basée pour le moment sur des processus physico-chimiques complexes et mal contrôlés, par des technologies plus robustes et prévisibles ;

– éviter la perte des compétences dans le privé et le public. Prendre les mesures urgentes nécessaires à la préservation des compétences clés, avant qu'elles n'aient complètement disparu de l'Europe ;

– favoriser l'innovation et l'apparition d'une offre industrielle de qualité. Soutenir vigoureusement les quelques entreprises qui ont déjà effectué des avancées vers la réalisation de disques optiques numériques enregistrables de très bonne longévité ;

– élaborer une véritable politique d'archivage numérique. S'assurer au sein de chaque ministère que les données numériques importantes sont bien l'objet du suivi indispensable à leur survie. Évaluer l'intérêt d'une mutualisation des moyens, dans la perspective d'une stratégie active à l'échelon national, ou de la création d'un centre de conservation des données numériques à long terme équipé de robots permettant le suivi nécessaire à grande échelle.

Les auteurs en appellent aux financements publics, notamment de la France, de l'Allemagne et des Pays-Bas en tant que principaux pays concernés par la focalisation de compétences clés, ainsi que de l'Union européenne.

En attendant que des réponses satisfaisantes soient apportées, les auteurs de l'étude conseillent de multiplier les sauvegardes grâce, au moins, à deux disques optiques et un disque dur magnétique, sans oublier de recommencer la procédure tous les quatre ans sur un support neuf.

Interrogé sur la protection des informations sur les serveurs de la BNF, M. Bruno Racine, lors de son audition du 1er décembre 2010, a rappelé que lorsqu'on avait procédé aux premières numérisations, la durée de vie des supports choisis était inférieure à la durée prévue du programme de numérisation lui-même ! Aujourd'hui, le système d'archivage de la BNF bénéficie d'une infrastructure stable et pérenne même si la qualité des documents mis en ligne, notamment les images, ne permet pas leur réutilisation commerciale.

Il a souligné que la question de la protection est plus centrale pour les œuvres non libres de droits. Mais dans ce cas, les fichiers ne sont pas accessibles et leur protection relève de la responsabilité des éditeurs.

3. La captation de la valeur par les grands acteurs du web au détriment de la production de contenus

Les grands moteurs de recherche structurent la manière dont les internautes accèdent aux contenus.

Ils sont devenus des intermédiaires incontournables pour des internautes en quête de contenu et d'information. Ces moteurs engendrent plus de 100 milliards de requêtes quotidiennes dans le monde, dont 70 % pour le seul *Google* (1). Avec une part de marché mondiale avoisinant les 70 % (90 % en France), *Google* a la maîtrise de la hiérarchisation des contenus quels qu'ils soient sur Internet et donc de leur accessibilité.

La puissance d'acteurs tels que *Google*, *Yahoo !*, *Microsoft* et *AOL*, qui ajoutent à leur position de « porte d'entrée » une gamme de services de plus en plus étendue, leur assure une position de force en terme d'accumulation d'audience et d'accroissement de leur part de marché publicitaire, sans les conduire à investir dans la production des contenus sans lesquels leur fonction d'orientation des internautes n'a plus lieu d'être.

Peu enclins à investir dans les contenus, car se présentant généralement comme des prestataires techniques, ces acteurs remettent en cause l'équilibre précaire de l'économie de la production de contenus :

– en « vampirisant » les sites éditoriaux – comme le dénoncent les acteurs de la presse écrite à travers le monde –, c'est-à-dire en utilisant leurs contenus pour attirer les audiences dans un premier temps puis en phagocytant cette audience en permettant de consulter tous les contenus depuis le même service (2) et, enfin, en valorisant ces audiences auprès des annonceurs au détriment des sites éditeurs originels des contenus ;

– en captant une part croissante des revenus publicitaires autrefois perçus par d'autres médias « traditionnels » qui assument les coûts de la production.

La question se trouve dès lors posée de savoir si leur développement ne risque pas d'entraîner une remise en cause du modèle économique des éditeurs et créateurs de contenus, notamment des médias traditionnels, qui participent au financement de la production. Comment éviter ce risque ?

---

(1) En France, la part de marché de Google sur les moteurs de recherche est de 87 % en juillet 2009 selon AT Internet institute.

(2) Sur ce modèle, Yahoo *a annoncé le 26 août 2009 le lancement de son service In-line player qui permet de lire un certain nombre de vidéos directement depuis la page de résultats des recherches, sans nécessiter d'être redirigé vers le site hébergeur (http://www.ysearchblog.com/2009/08/26/video-search-enjoy-largeNn-line-play-and-embedded-related-videos/).*

Parfois envisagée afin de remédier à cette absence d'investissement des portails, la mise en place d'obligations de financement de la production par les portails nécessiterait sans doute en raison de leur caractère international une action concertée au plan mondial, ou au moins européen.

En effet, si les éditeurs de portails disposent de filiales nationales sur les marchés européens majeurs (18 filiales européennes pour *Google* et AOL), leurs sièges sociaux sont domiciliés aux États-Unis et leurs bureaux « Europe » dans des pays autres que la France (Irlande pour *Google* et *AOL*, Royaume-Uni pour *Yahoo !* et Pays-Bas pour *Microsoft*).

Compte tenu de la localisation juridique très variable des portails, il semble difficile de les taxer directement ou de leur imposer des obligations d'investissement dans la production. Les ressources de ces services émanant directement de la publicité, il avait été proposé, notamment par le rapport, remis en janvier 2010, de la mission « création et internet » présidée par M. Patrick Zelnik, président-directeur général de Naïve, de taxer les investissements publicitaires des annonceurs français sur ces portails. C'est la philosophie qui sous-tend la taxe dite « *Google* » fixée à 1 % « sur l'achat des services de publicité en ligne », adoptée en loi de finances initiale pour 2011 mais dont l'entrée en vigueur était prévue au 1er janvier 2011 et qui, dans le cadre de l'examen du projet de loi de finances rectificative pour 2011 à l'Assemblée nationale, a été supprimée par un amendement de Mme Laure de La Raudière, ce projet de loi de finances n'étant pas définitivement adopté à ce jour.

Un phénomène du même ordre pourrait se produire avec l'avènement de la télévision connectée, qui donnera indifféremment accès au monde de l'Internet et de la télévision sur un même téléviseur, mais dont nul ne sait encore précisément à quel rythme elle va se développer ni les bouleversements qu'elle va entraîner. Les chaînes de la TNT gratuite redoutent surtout que les grands acteurs du Web, tels *Google* ou *Yahoo*, ne viennent les concurrencer sur leur terrain. *Google* aurait par exemple l'intention d'utiliser *YouTube* pour lancer 20 chaînes « premium » accessibles uniquement sur la télévision connectée. Avec leur puissance financière, les géants du Net pourraient même acheter les productions des studios de Hollywood. Apple ou *Google* seraient en mesure d'acquérir la totalité des droits des séries et des films des studios américains Ces entreprises pourraient capter une part importante des investissements publicitaires, alors même qu'elles ne sont pas soumises à la même réglementation que les chaînes de télévision, en particulier les obligations de financement de la création.

Pour se protéger, les 18 principales chaînes de télévision françaises ont signé, en novembre 2010, une charte dans laquelle elles s'engagent à garantir l'intégrité et le contrôle des contenus sur ces téléviseurs.

Si l'usage du téléviseur connecté venait à se généraliser, le secteur audiovisuel, qui connaît une situation de fragilité, serait inévitablement bousculé. La chaîne de valeur sera là encore menacée. Potentiellement, la télévision

connectée est une bombe à fragmentation de l'audience et comporte un risque fort de contournement pour certains acteurs traditionnels, en particulier les chaînes et les distributeurs, avec pour conséquence un affaiblissement des diffuseurs dont les recettes publicitaires diminueront, ce qui menacera le financement des films et de la production audiovisuelle. Il faut donc agir préventivement en cherchant les moyens d'assurer un équilibre entre acteurs traditionnels du secteur et nouveaux acteurs tant en termes d'accès à la ressource publicitaire que de participation au financement de la création.

Orientation n° 5 : garantir une répartition équitable de la valeur entre les grands moteurs de recherche et les agrégateurs de contenus d'une part et les médias traditionnels et producteurs de contenus d'autre part

Si un mécanisme permettant de taxer les recettes publicitaires des grands moteurs de recherche, type taxe « *Google* », venait à entrer en vigueur, il serait souhaitable d'inciter nos partenaires européens à instituer un même mécanisme de taxation, afin de ne pas pénaliser les annonceurs français et d'accroître l'efficacité de cette mesure.

Pour éviter que la télévision connectée ne fragilise trop les chaînes de télévision qui font l'objet d'une régulation importante et participent largement au financement de la création, il convient de conduire rapidement une réflexion sur les moyens d'assurer un équilibre entre acteurs traditionnels du secteur et nouveaux acteurs, tant en termes d'accès à la ressource publicitaire que de participation au financement de la création.

La mise en place d'obligations de financement de la production par les portails web nécessiterait en raison de leur caractère international une action concertée au plan mondial, ou au moins européen.

DEUXIÈME PARTIE : INTERNET, UN NOUVEL INSTRUMENT AU SERVICE DE LA DÉMOCRATIE

I. INTERNET : UN CATALYSEUR DU DÉBAT DÉMOCRATIQUE

Les conséquences de l'usage généralisé d'Internet sur les droits politiques sont manifestes. Aujourd'hui, ce média fait à ce point partie des moyens d'expression fondamentaux que toute tentative pour le contraindre est interprétée comme un signe d'arbitraire. Le Web n'a pas seulement élargi à l'ensemble de la planète le lectorat des médias traditionnels mais a permis à chaque individu, pour peu qu'il ait accès au réseau, de participer pour son propre compte à un échange universel d'informations. Les nouvelles formes de communication que les techniques numériques ne cessent d'engendrer, comme les réseaux sociaux, les blogs ou le microbloging, ont ainsi transformé Internet en un instrument de contre-pouvoir dont l'efficacité a pu être prouvée à plusieurs reprises. Témoigner [(1)], s'organiser, résister sont autant d'engagements qui passent de plus en plus par le vecteur de la communication électronique. Comme a pu le dire le militant chinois Chen Guangcheng « *L'Internet,* Twitter*, les blogs ont doté les citoyens de leur propre voix*. » [(2)]

L'actualité parle d'elle-même. Il a suffi pendant les travaux de la mission d'information d'être à l'écoute des événements internationaux pour constater les conséquences politiques d'une utilisation militante d'Internet. Sans doute, il serait difficile d'affirmer que les soulèvements populaires qu'ont connus, par exemple, la Tunisie et l'Égypte, doivent tout à Internet ; mais le recours au Web a contribué à contourner les moyens de répression des régimes contestés [(3)] et a donné un impact international aux luttes engagées.

Quand sont invoquées, pour poser des limites à cette liberté, non pas d'autres droits légitimes de la personne mais les notions de sécurité d'État ou d'ordre public, toutes les dérives sont ouvertes. La censure peut prendre des formes variées : bloquer l'accès à un site, rendre inaccessibles certains résultats de recherche par mots clés, voire interrompre l'accès au réseau. Les pays recourant systématiquement à ces techniques sont régulièrement dénoncés, les plus cités étant la Chine, la Birmanie, la Corée du Nord, Cuba, l'Iran, l'Ouzbékistan, la Syrie, le Turkménistan, le Viêt Nam et le Belarus.

---

(1) Certaines vidéos postées sur YouTube *ont eu une répercussion internationale. La plus connue reste celle d'une jeune femme iranienne, tuée d'une balle pendant une manifestation à Téhéran, le 20 juin 2009.*

(2) Le nouveau défi de M. Chen, Le Monde*, 9 mars 2011.*

(3) Les premières manifestations en janvier 2011 en Égypte se sont faites à l'appel du cyberdissident Waël Ghonim par le biais de Facebook*. Waël Ghonim était par ailleurs chef du marketing de* Google *au Proche Orient et en Afrique. Il a été emprisonné du 27 janvier au 8 février 2011. (Source :* Le Monde*, 10 février 2011).*

Une des formes les plus sévères de censure est la tentative de morceler le Web mondial en créant des zones d'intranet indépendantes et plus aisées à contrôler.

Ce sont enfin les internautes eux-mêmes qui peuvent être persécutés. L'ONG *Reporters sans frontières* a décompté, en 2010, 120 blogueurs, internautes et cyberdissidents emprisonnés, majoritairement en Chine, au Viêt Nam et en Iran.

Les États-Unis se sont particulièrement engagés dans l'aide aux internautes défenseurs des droits de l'homme. Certains d'entre eux ont pu bénéficier de formations à des technologies permettant de contourner les blocages du Web, de sécuriser les échanges d'informations et de parer les cyberattaques contre les sites militants. Depuis 2009, 50 millions de dollars ont été consacrés à ces programmes par l'administration du Président Barack Obama.

Chaque acte de répression montre *a contrario* le pouvoir que représente Internet dans la défense des libertés des individus. Les crises politiques sont désormais abordées du point de vue de leurs conséquences sur la liberté de communication par voie numérique. Caractéristique de cet état des choses a été la première réaction de Mme Hillary Clinton, chef du département américain des affaires étrangères, appelant, au début de la crise en Égypte, les autorités égyptiennes à *« mettre fin aux mesures sans précédent qu'elles [avaient] prises pour bloquer les communications* ».

Dans une tribune [(1)] publiée le 10 mai 2010, M. Bernard Kouchner, alors ministre des Affaires étrangères, a rappelé que cette question n'opposait pas l'Occident au reste du monde ; la preuve en est que « *180 États réunis dans le cadre du Sommet mondial sur la société de l'information ont reconnu la pleine applicabilité à Internet de la Déclaration universelle des droits de l'homme, en particulier de l'article 19 qui établit la liberté d'expression et d'opinion.* » [(2)]

Le Sommet mondial sur la société de l'information avait été organisé à l'initiative de l'ONU en application d'une résolution adoptée par l'Assemblée générale le 31 janvier 2002. Deux réunions ont eu lieu : à Genève en décembre 2003 et à Tunis en novembre 2005.

Depuis, le cours de l'histoire a conféré une valeur nouvelle à Internet ; les chefs d'État et de gouvernement du G8, réunis à Deauville les 26 et 27 mai 2011, en ont solennellement pris acte et se sont engagés « *à encourager l'utilisation d'Internet comme instrument de promotion des droits de l'homme et de la participation démocratique dans le monde entier.* » [(3)]

Dans le prolongement de cette initiative, il serait souhaitable que la défense de cet outil de communication fasse l'objet d'un engagement renouvelé de

(1) Le Monde*, 10 mai 2010*
(2) Engagement de Tunis, 18 novembre 2005.
(3) Déclaration du G8 de Deauville, 26-27 mai 2011, § 13.

l'ensemble de la communauté internationale ; l'ONU pourrait ainsi passer à une étape plus solennelle en proposant à ses membres le vote d'une déclaration qui reconnaîtrait la portée de ce nouvel espace de communication au regard des droits de l'homme.

Orientation n° 6 : **obtenir un engagement solennel de l'ONU reconnaissant la valeur d'Internet pour la promotion des droits de l'homme**

Engager une action diplomatique visant à l'adoption par l'ONU d'une déclaration sur la liberté de communication par voie électronique au regard de l'importance acquise par ces techniques pour la défense et la promotion des droits de l'homme.

II. LA *E*-DÉMOCRATIE EST-ELLE UNE NOUVELLE FORME DE DÉMOCRATIE ?

Dans quelle mesure ce nouveau média qu'est Internet contribue-t-il à la diffusion des valeurs démocratiques ? Internet est-il un outil venant compléter et renforcer les procédures traditionnelles de débat ou doit-on y voir l'amorce d'une transformation des conditions mêmes du débat démocratique devant conduire à de nouvelles façons de penser la prise de décision politique ?

En faveur de la première thèse, on constate que la portée de cette nouvelle technologie s'apprécie par les juges au regard des droits fondamentaux classiquement reconnus. Parce que la décision prise par le Conseil constitutionnel le 10 juin 2009 est fondamentale sur cette question, on rappellera les développements faits dans la première partie du présent rapport. Le Conseil constitutionnel a jugé « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions »,* la liberté d'accéder à Internet était impliquée parce que la Déclaration des droits de l'homme et du citoyen de 1789, en son article 11, a qualifié comme l'un des droits « *les plus précieux de l'homme* », à savoir « *la libre communication des pensées et des opinions* » [(1)].

Ce fondement juridique garantit à lui seul le libre développement des possibilités les plus récentes d'Internet. Ce média doit, en effet, être reconnu non seulement dans sa dimension « passive », portant sur l'accès à l'information, mais aussi dans sa dimension « active » : « *[…] Internet permet l'exercice de la liberté de communication dans laquelle le citoyen est émetteur d'information (dimension « active »). Le courrier électronique, le Web 2.0, les blogs… sont autant de formes contemporaines de la liberté de s'exprimer et de communiquer.* » [(2)]

(1) Décision n° 2009-580 DC du 10 juin 2009.
(2) Les Cahiers du Conseil constitutionnel*, n° 27, p. 7.*

Que l'utilisation d'Internet soit appréhendée au regard d'un des droits « les plus précieux de l'homme » justifie, précisément, la vigilance qu'il convient d'observer face à toute tentative d'en censurer l'usage.

Les différents mouvements politiques qui ont eu massivement recours à Internet pour organiser des actions de révolte l'ont fait dans une finalité traditionnelle de lutte contre des régimes ne respectant pas les droits de l'homme.

Certains défenseurs de la notion de *e-démocratie* portent cependant une ambition plus large. Internet ne serait pas seulement un nouveau support d'information et d'expression s'ajoutant à ceux que l'on connaît déjà, et méritant à ce titre de bénéficier de la même garantie d'accès que les autres, mais constituerait un moyen de transformation des conditions mêmes de l'activité politique tant au plan social qu'au niveau des procédures de décision. On prête ainsi à Internet la vertu de « créer du lien social », de faciliter l'« inclusion » de l'individu dans des groupes et de permettre l'émergence d'une « citoyenneté augmentée », selon une expression reprise des réflexions sur les biotechnologies.

La communauté des internautes viendrait concurrencer la communauté réelle, attirant à elle les mécanismes du pouvoir politique et imposant peu à peu ses procédés de légitimation.

Le point de départ de ces analyses est le constat qu'Internet offre des outils de communication faciles d'utilisation, disponibles 24 heures sur 24 et accessibles en tout lieu. Reliés au réseau, les utilisateurs peuvent créer des « espaces de dialogue », collaborer pour construire des arguments grâce aux divers outils du Web 2.0, sans qu'aucune de ces initiatives ne soit liée à une institution ou à un calendrier politique fixé d'avance. L'initiative de mobiliser les internautes citoyens autour d'un thème d'action peut survenir à tout moment et provenir de tout point du Web.

Les réseaux sociaux agrègent, quant à eux, les volontés au gré des affinités et constituent des forces de mobilisation spontanées. En outre, une fois constitués, ils sélectionnent pour leurs propres membres la multiplicité des informations disponibles sur Internet ; la fonction « j'aime » proposée par *Facebook* crée des sphères culturelles autonomes.

Chaque individu pouvant participer anonymement à une multiplicité de réseaux sociaux différents, la notion de personne s'estompe au sein de collectifs ou de communautés aux contours souples, toujours adaptables à de nouveaux objectifs. Rapidité, multiplicité, universalité, feraient d'Internet non seulement l'agora des temps modernes ou la réalisation de l'idéal de l'échange libre et transparent des arguments, mais un outil de remise en cause permanente des instances légitimes.

Si la politique est l'art dont la finalité est le bonheur de la communauté, Internet serait l'instrument le plus adapté à cette fin qui ait jamais été conçu : « *le*

bonheur est dans le binaire » a pu affirmer M^e^ Alain Bensoussan, avocat à la cour d'appel de Paris au cours de son audition devant la mission d'information [(1)].

La conception selon laquelle Internet introduirait une citoyenneté radicalement nouvelle a pu faire l'objet de critiques sévères. Dès 2003, l'OCDE faisait part de son scepticisme : « *Le leurre de la démocratie directe, à demi-libertaire et populiste et à demi-rousseauiste, a servi à enraciner le projet dans le royaume du politiquement naïf et du nostalgique. Au lieu de chercher à mettre les technologies numériques au service de la démocratie existante, les pionniers à vision hautement spéculative et futuriste de la démocratie en ligne donnèrent l'impression de tabler sur l'implosion des constitutions et des institutions face au nouveau paradigme numérique.* » [(2)]

Loin de renforcer la participation des individus à la vie de la collectivité, certaines données tendraient à montrer qu'Internet aurait plutôt pour effet de réduire le champ de l'action politique aux personnes les plus engagées et d'en distraire les autres. Les résultats d'une enquête menée en 2009 confirment, selon M. Thierry Vedel, un constat déjà fait aux États-Unis : « *l'essor de l'Internet et la multiplication des chaînes de télévision non généralistes permettent à ceux qui s'intéressent peu à la politique de s'en détourner encore plus, et tendent à accroître la polarisation des citoyens politisés. L'Internet semble donner plus de ressources et d'espaces d'expression aux citoyens qui sont déjà les mieux intégrés dans le système politique*. » [(3)]

Si la constitution de réseaux sociaux peut être un moyen très puissant pour fédérer un mouvement de contestation, elle pourrait aussi avoir des effets de fermeture ou de repliement vers des positions de désengagement politique. En faisant un usage hyperbolique de la notion d'amitié et en créant des communautés fondées uniquement sur des affinités, le réseau social ne favoriserait pas l'échange d'arguments différents ni d'éléments culturels diversifiés. Comme l'a expliqué, d'un point de vue plus général, M. Dominique Wolton, un échange d'informations ne constitue pas une communication, laquelle exigera toujours conflits et contraintes [(4)].

Il n'en demeure pas moins que l'action politique est, de fait, sous l'influence du nouveau contexte numérique, comme l'ont confirmé les participants à la table ronde organisée par la mission d'information sur le monde numérique et la démocratie locale [(5)]. Ainsi, en contribuant à la transparence de l'action des élus locaux, Internet aurait modifié les rapports entre les élus et leurs administrés, du moins ceux qui sont familiers du Web. Selon M. Marc-Antoine Jamet, représentant de l'association des maires de France, on assisterait, actuellement, à « *une mise en concurrence de l'administration municipale* ». La multiplication de

(1) Audition du 27 octobre 2010.

(2) Promesses et limites de la démocratie en ligne*,* les défis de la participation citoyenne en ligne*, OCDE, 2003, p. 163.*

(3) Thierry Vedel, « Internet creuse la fracture civique », Le Monde*, 22 juin 2010.*

(4) Audition du 30 juin 2010.

(5) Audition du 8 décembre 2010.

sites privés ou créés par des associations, ainsi que la mise en ligne de nombreux blogs, fait que « *tout le monde devient commentateur, journaliste ou expert*. » L'information en continu se double ainsi d'un contrôle en continu entraînant, selon les termes de M. Fabrice Dalongeville, représentant de l'association des maires ruraux de France, « *un processus référendaire permanent* » qui aurait entraîné une perte de légitimité de l'élu.

Au vu de ces positions très contrastées, la mission d'information a abordé ces questions d'un point de vue pragmatique en considérant ce que la « démocratie existante » avait à gagner en encourageant les médias numériques. Évaluant la richesse et l'inventivité de ces nouvelles modalités d'expression démocratique, elle en a également constaté les difficultés d'usage, qui renvoient, semble-t-il, à des problèmes de méthode et d'évaluation.

III. QUE RECOUVRE LE TERME DE *E*-DÉMOCRATIE ?

La recommandation du Comité des ministres du Conseil de l'Europe du 18 février 2009 dessine comme suit les contours de la notion de *e-démocratie* : « *La démocratie électronique englobe en particulier le parlement électronique, la législation électronique, la justice électronique, la médiation électronique, la cyberécologie, l'élection électronique, le référendum électronique, l'initiative électronique, le vote électronique, la consultation électronique, la pétition électronique, les campagnes électroniques, le sondage électronique et l'enquête électronique ; elle a recours à la participation électronique, à la délibération électronique et aux forums électroniques.* » [(1)]

Si les impacts des outils numériques sont multiples et touchent peu à peu tous les moyens d'expression démocratique, les divers champs concernés peuvent cependant se rassembler autour des trois moments qui marquent un processus démocratique : l'information, la délibération et la décision.

A. UN CITOYEN MIEUX INFORMÉ

La mission d'information s'est en particulier intéressée aux sites d'information institutionnels qui ont été créés dans le but d'éclairer le citoyen sur les affaires publiques, tant dans le cadre national que local.

1. Être mieux informé sur les débats menés au niveau national

À l'échelon national, les deux assemblées du Parlement sont dotées de sites Internet sur lesquels l'ensemble des travaux, tant en séance plénière qu'en commissions, est maintenant accessible.

---

(1) Principe 35 de la recommandation CM/Rec (2009)1 du Comité des ministres aux États membres sur la démocratie électronique, adoptée par le Comité des ministres le 18 février 2009.

Concernant l'Assemblée nationale, tous les débats depuis le 1er juin 1958 et l'ensemble des questions écrites posées par les députés depuis cette date ont été numérisés et mis en ligne.

Les débats en séance sont retransmis en direct et archivés sous forme de vidéos à la demande. Un nombre croissant de réunions de commissions et de missions d'information bénéficie d'une retransmission vidéo.

Le site de l'Assemblée nationale compte plus de 800 000 visites par mois.

Des forums et des blogs sont ouverts sur le site du Sénat.

Une prise en compte des avis des internautes sur les études d'impact qui sont annexées aux projets de loi depuis l'adoption de la loi constitutionnelle du 23 juillet 2008 et l'entrée en vigueur de la loi organique n° 2009-403 du 15 avril 2009 est prévue par les articles 83 et 86 du Règlement de l'Assemblée nationale. Les documents évaluant les conséquences de chaque projet sont mis à disposition par voie électronique afin de recueillir toutes les observations. Les contributions sont transmises aux rapporteurs qui doivent les présenter à l'ensemble de leurs collègues dans une annexe à leur rapport.

On soulignera, par ailleurs, une initiative particulièrement remarquable prise par le Conseil constitutionnel consistant à retransmettre, sous forme vidéo sur son site Internet, les audiences publiques tenues dans le cadre de la procédure des questions prioritaires de constitutionnalité. Le président du Conseil a la faculté d'en ordonner la diffusion après avoir recueilli l'avis des parties présentes [(1)]. La large publicité ainsi assurée à ces audiences par le biais d'Internet donne toute sa portée à cette importante réforme juridique.

Les sites Internet du Conseil constitutionnel, du Conseil d'État et de la Cour de cassation assurent aussi une information juridique complète, tant sur les dernières décisions rendues qu'en matière de jurisprudence.

De nombreux sites Internet présentent l'activité du pouvoir exécutif. Le site de la présidence de la République rend compte des déplacements et des rencontres du Président de la République et rend accessibles tous ses discours, ses déclarations et ses interviews. Le traditionnel service du courrier au Président peut-être saisi par voie électronique ; le site « *Écrire au Président de la République* » propose un formulaire permettant la rédaction de messages auxquels il est répondu par voie postale ou sous forme de courrier électronique.

Le portail du Gouvernement offre des fonctionnalités similaires. Un formulaire de courrier au Premier ministre est mis en ligne, les messages envoyés étant ensuite traités par le service des interventions.

---

(1) Cf. article 9 de la décision du 4 février 2010 portant règlement intérieur sur la procédure suivie devant le Conseil constitutionnel pour les questions prioritaires de constitutionnalité.

Enfin, chaque département ministériel dispose de son site Internet. En plus d'informations sur les activités propres à chaque ministre, ces sites présentent l'organisation des ministères et, notamment, de nombreux dossiers de renseignements ainsi que des formulaires administratifs.

2. Être mieux informé sur les débats menés au sein des collectivités territoriales

La mission d'information a pu constater la réalité d'un phénomène pouvant apparaître comme un paradoxe. L'utilisation la plus engagée d'Internet par les citoyens se fait moins dans le cadre du « village global » qu'à un niveau local, celui du village, du quartier, de la ville, du département ou de la région. Des réseaux sociaux, tels que le réseau *Peuplade.fr*, se sont même constitués à l'échelle des quartiers. Contredisant l'utopie d'un cyber espace sans ancrage géographique ni racine culturelle, l'expérience que les élus locaux ont de l'outil numérique est que celui-ci a modifié les conditions dans lesquelles les problématiques les plus proches des citoyens sont débattues.

Selon une enquête publiée par l'association des maires de France [(1)], le taux de collectivités dotées d'un site Internet serait de 90 % pour les intercommunalités en zone urbaine et de 68 % en zone rurale. 40 % des communes seraient équipées.

Ce taux se réduirait à 25 % pour les petites communes, selon M. Fabrice Dalongeville intervenant devant la mission au nom de l'association des maires ruraux de France. Certains maires peuvent en effet s'interroger sur la nécessité de créer un site Web communal, surtout si la commune est très petite. Rien ne les contraint, évidemment, à mettre en place un tel outil de communication.

L'intérêt croissant des citoyens pour Internet devrait néanmoins, selon M. Fabrice Dalongeville, conduire à stimuler la création de sites Internet, la perspective du renouvellement des mandats en cours servant aussi d'aiguillon.

Un autre élément incitatif est la prise en compte croissante de l'économie du tourisme. Internet est un moyen peu onéreux pour une commune de faire connaître sur une grande échelle son territoire et son histoire.

a) Les difficultés pour créer et gérer un site Internet d'une collectivité territoriale

La création et la gestion d'un site Internet représentent une lourde tâche pour les petites communes. Selon l'enquête précitée, les difficultés sont de deux ordres.

En premier lieu, la fracture numérique entre les territoires se marque encore par le fait que 10 % des mairies ne disposent que d'une connexion à bas

(1) Enquête communes et technologies de l'information et de la communication, IDATE, octobre 2010.

débit. Si la majorité des mairies bénéficie de débits entre 512 kbps et 2 Mbps, le développement de nouvelles applications, comme par exemple la vidéo, exigerait des capacités de flux supérieures.

En second lieu, se pose un problème de compétence. Comme l'ont souligné les participants à la table ronde organisée par la mission d'information sur le rôle joué par Internet sur la démocratie locale (1), la gestion d'un site repose souvent sur l'enthousiasme d'un agent de mairie ou d'un adjoint. Un tiers des communes de moins de 5 000 habitants délèguent cette mission à un élu en marge de ses fonctions municipales (2).

Pour répondre à ce défi, M. Fabrice Dalongeville, a appelé à la constitution d'équipes de « hussards du numérique », constituées des maires et des professeurs des écoles. Les bâtiments scolaires pourraient être utilisés à cette fin en dehors des heures de cours.

L'enquête précitée souligne l'effet levier qu'a eu, pour le développement des compétences, le programme « écoles numériques rurales » lancé en 2009 par le ministère de l'Éducation nationale. Les subventions accordées à cette occasion – 67 millions d'euros en 2009 – ont donné les moyens aux communes, notamment aux plus petites, de mieux s'impliquer dans le monde du numérique en investissant dans des programmes informatiques à destination du monde éducatif. 6 700 communes ont bénéficié du programme lancé en 2009 ; 6 593 écoles ont été retenues en 2011, le ministère de l'éducation nationale assurant le financement du matériel informatique et la commune celui de la mise en réseau. Il est regrettable, cependant, que ce plan n'ait pas vu ses fonds accrus pour 2011, comme de nombreux acteurs engagés dans le développement d'Internet le demandaient.

Parmi les quelques initiatives prises pour aider les mairies à se doter d'un site Web, le projet *Campagnol,* lancé par l'association des maires ruraux de France, se distingue par sa simplicité. Il consiste à fournir des sites Internet « clés en mains » pour la somme de 180 euros. Ce projet propose un hébergement sécurisé des données, une partie de l'information étant collectée localement, une autre mutualisée.

b) Les services proposés par les sites Web des communes

Les sites Web communaux proposent trois services de base : une information sur les débats et les décisions du conseil municipal ; des services administratifs en ligne ; des renvois aux sites des associations.

Il est également de plus en plus fréquent d'y trouver une plateforme dématérialisée des marchés publics et des systèmes d'information géographique.

(1) Audition du 8 décembre 2010.
(2) Cf enquête précitée.

La présence d'outils plus collaboratifs est moins répandue. Des services comme les rendez-vous en ligne avec les élus sont rarement mis en place, selon l'enquête précitée ; celle-ci constate également que *« l'inscription ou la réservation en ligne (crèche, bibliothèque, transport…) ne concernerait que 8 % des sites, ce pourcentage diminuant encore pour les sites transactionnels permettant le paiement en ligne.* »

Les services de *e-administration* se réduisent souvent à la possibilité de télécharger des formulaires administratifs.

Près de 300 communes proposent sur leur site deux services pilotes : l'inscription en ligne sur les listes électorales et le recensement citoyen.

De plus en plus de communes disposent enfin d'un compte *Twitter* ainsi que d'un compte *FaceBook*.

LE LABEL VILLE INTERNET

L'association Villes Internet promeut le développement de « l'Internet citoyen ». Ses actions portent sur le développement :

« – des sites de villes, pour être en relation avec sa municipalité et accéder aux données publiques, aux droits, aux services administratifs ;

« – des espaces citoyens, pour réfléchir ensemble : pages d'association, ou de citoyens actifs ;

« – des réseaux sociaux numériques, pour amplifier les réseaux humains existants et se connaître, échanger,

« – tous les usages des outils numériques mobiles, qui permettent de mieux investir sa ville ou son village. *»* [(1)]

L'association remet des labels Ville Internet. Cinq niveaux de labellisation sont reconnus. Depuis 1999, 2 222 labels ont été décernés à 774 collectivités locales. Le palmarès 2011 a distingué 303 villes.

Une double contrainte pèse sur les élus : répondre à la légitime demande de transparence de leurs administrés accoutumés à l'usage d'Internet et s'adapter à des outils en constante évolution.

(1) Cf. http://www.villes-internet.net/

Pour soutenir l'engagement des élus locaux dans la *e-démocratie* il conviendrait que l'ensemble des administrations centrales chargées du développement des services Internet de l'État [(1)] fassent un plus grand effort d'information envers les élus locaux et partagent leur expérience.

Certes, la direction générale de la modernisation de l'État (DGME) explique qu'elle va régulièrement « *au contact des communes pour leur présenter les différents services en ligne qui leur sont proposés. Le processus de raccordement est simple et les communes sont accompagnées durant l'opération. Lors du raccordement, nous fournissons aux communes :*

« – des éléments d'information leur permettant de mieux comprendre les démarches en ligne (FAQ, documentation technique, outils de communication, plaquette d'information concernant mon.service-public.fr*) ;*

« – des éléments d'auto-formation leur présentant les démarches vues de l'usager et vues du service instructeur ainsi que le déroulement du raccordement proprement dit, accompagnés d'une FAQ ;

« En termes de supports, les communes raccordées ont également la possibilité de contacter la DGME par mail *ou par téléphone.* » [(2)]

En l'absence, cependant, d'évaluation du nombre de communes qui entrent effectivement en contact avec la DGME, il est difficile d'apprécier la portée de cette aide. De nombreux élus semblent, en tout état de cause, ne pas être informés de l'existence de tels services.

Si l'on considère que ces sites contribuent à la vie de la démocratie locale, il conviendrait qu'un effort plus systématique soit fait pour encourager leur création ; à défaut, les droits des citoyens s'exerceront d'une manière de plus en plus différenciée selon les territoires.

Orientation n° 7 : développer les sites Web des communes

Engager les services des administrations centrales compétentes à mieux informer les maires sur les conditions dans lesquelles ceux-ci peuvent créer, gérer et faire évoluer les sites Web communaux de sorte que tous les citoyens, en tout lieu du territoire national, puissent disposer, à égalité, des nouveaux outils numériques de démocratie locale.

3. Garantir que les sites Internet des collectivités territoriales reflètent le débat démocratique

Si l'on estime nécessaire de reconnaître qu'Internet peut remplir une fonction importante dans la vie de la démocratie, il semblerait que le minimum que l'on puisse attendre des sites Web des collectivités locales soit qu'ils rendent

(1) Direction générale de la modernisation de l'Etat (DGME), direction de l'information légale et administrative (DILA), et délégation aux usages de l'Internet (DUI).

(2) Réponse à un questionnaire adressé à la DGME par la mission d'information.

compte de manière transparente des débats tenus au sein des assemblées délibérantes. Avant de lancer une réflexion sur une nouvelle forme de démocratie spécifique à la sphère des internautes – et dont on apprécie mal les contours – il conviendrait certainement de se concentrer sur la forme traditionnelle, et seule reconnue, du débat démocratique qui est celle d'une discussion entre une majorité et une opposition dont les citoyens doivent pouvoir être informés.

a) Les comptes rendus des débats sur les sites Internet des collectivités territoriales

Les articles L. 2121-18, L. 3121-11, L. 4132-10 et L. 5912-2 du code général des collectivités territoriales disposent que les séances des assemblées délibérantes locales peuvent être retransmises par les moyens de communication audiovisuelle.

La mise à disposition des délibérations exécutoires ne peut cependant se faire que sous réserve de rendre anonymes les données personnelles communiquées au cours des débats (1).

On constate que lorsqu'une collectivité locale est dotée d'un site Internet, les comptes rendus écrits des réunions sont, le plus souvent, mis en ligne.

La présentation plus ou moins détaillée des différentes initiatives et projets de la collectivité complète, en général, la bonne information des administrés.

Ces différents contenus reflètent cependant mal les débats réels qui peuvent être soulevés dans les assemblées délibérantes.

Ainsi, les interventions des élus de l'opposition peuvent ne pas figurer dans les procès-verbaux des réunions. Au regard de la jurisprudence, il suffit en effet que le procès-verbal fasse « *apparaître la nature de l'ensemble des questions abordées au cours de la séance* » (2) et n'a pas à faire mention des interventions des conseillers municipaux (3). La mise en ligne des procès-verbaux des réunions des assemblées délibérantes ne garantit donc pas la publicité des positions défendues par l'opposition.

Certains sites rendent certes accessibles les retransmissions vidéo des séances mais le coût d'un tel service le réserve à quelques très grandes collectivités dès l'instant où le visionnage se fait à la demande.

b) Le droit d'expression des élus de l'opposition

Le droit d'expression des élus sur les supports d'information édités par les communes est légalement garanti par les dispositions de l'article L. 2121-27-1 du code général des collectivités territoriales aux termes desquelles : « *Dans les*

(1) Cf. réponse à la question écrite n° 65487 (Assemblée nationale) de M. Bernard Roman.
(2) CE, n° 145597, 27 avril 1994.
(3) CE, n° 75312, 18 novembre 1987.

communes de 3 500 habitants et plus, lorsque la commune diffuse, sous quelque forme que ce soit, un bulletin d'information générale sur les réalisations et la gestion du conseil municipal, un espace est réservé à l'expression des conseillers n'appartenant pas à la majorité municipale. Les modalités d'application de cette disposition sont définies par le règlement intérieur. » Des dispositions équivalentes s'imposent aux conseils généraux, aux conseils régionaux et aux établissements publics de coopération intercommunale (EPCI) comprenant au moins une commune de 3 500 habitants et plus [(1)].

L'application de cet article aux sites Web a été précisée par un arrêt de la cour administrative d'appel de Versailles en date du 17 avril 2009. En conséquence de cette jurisprudence, un site Web d'une mairie peut être considéré, en lui-même, comme un bulletin d'information générale dès le moment où y sont exposés les réalisations et les projets de l'assemblée délibérante : « *la circonstance que [la commune] publie un magazine où les élus locaux de l'opposition peuvent exercer leur droit d'expression ne l'exonère pas de l'obligation de réserver un espace à cet effet [...] dans les autres bulletins d'information générale éventuellement diffusés à son initiative*. » Si le site Internet peut être regardé, eu égard à son contenu, comme constituant un bulletin d'information générale, alors un espace doit y être réservé à l'expression des conseillers n'appartenant pas à la majorité municipale.

En d'autres termes, il ne suffit pas que le bulletin d'information papier, traditionnellement édité et dans lequel, par ailleurs, l'opposition doit pouvoir s'être exprimée, soit numérisé et mis en ligne pour qu'il puisse être considéré que les élus de l'opposition disposent d'un espace d'expression sur le site Internet de la collectivité. Sur celui-ci doit leur être garanti, en outre, un espace spécifique d'expression dès lors qu'y sont diffusées des informations mettant en valeur les actions de la majorité.

c) Des obligations légales mal adaptées

Il convient néanmoins de reconnaître que la disposition de l'article L. 2121-27-1 précité a été rédigée dans la seule perspective de l'édition d'un document papier paraissant sous forme de bulletin. Or un site Web organise ses informations d'une tout autre façon. Il s'ordonne, notamment, selon une hiérarchie de répertoires permettant d'éditer une variété d'informations faisant l'objet de mises à jour différenciées. Quelles sont les informations et les rubriques qui doivent ouvrir un droit de réponse de l'opposition ? Comment coordonner la date de mise en ligne des différentes interventions des élus ?

En outre, de par sa structure, un site Web distribue ses contenus en niveaux différents ; certaines informations ne deviennent donc accessibles depuis la page d'accueil qu'après que l'internaute a cliqué sur plusieurs liens. À quel

(1) Cf. articles L. 3121-24-1, L. 4132-23-1 et L. 5211-1 du code général des collectivités territoriales.

degré de profondeur de recherche convient-il que les interventions de l'opposition soient consultables ?

Enfin, le contenu d'un site Web peut être interprété diversement. Certains sites sont essentiellement descriptifs. Des bilans ponctuels y sont faits sur diverses questions, la partie « services » étant prédominante. D'autres sont plus dédiés à la mise en valeur de l'action et des initiatives de l'assemblée concernée.

Ces interrogations expliquent certainement pourquoi peu de collectivités locales se conforment aux exigences légales telles qu'elles ont été précisées par le juge. Elles sont cependant un certain nombre à l'avoir fait, soit de leur propre initiative soit à la suite d'une saisine de l'autorité préfectorale dans le cas où celle-ci se justifiait.

d) Les tribunes de l'opposition sur les sites Web

La consultation des sites Web des dix communes les plus peuplées de France montre que deux d'entre elles, Nice et Strasbourg, accordent sur leurs sites un espace d'expression à l'opposition, intitulé « Tribune de l'opposition » (1) pour la première et « Tribune d'expression » (2) pour la seconde.

Plusieurs communes de taille plus réduite ont pris la même initiative. Les « tribunes d'expression » sont réservées aux groupes ou aux membres isolés de l'opposition mais sont quelquefois ouvertes à l'ensemble des élus. Elles sont généralement accessibles à partir d'un onglet placé dans la rubrique « Vie municipale ». Leur contenu prend la forme de prises de position ou renvoie aux sites politiques et aux blogs gérés par les groupes. Ce droit d'expression est reconnu par le règlement intérieur du conseil municipal.

Pour renforcer le débat démocratique sur les sites Internet des collectivités, la mission d'information suggère que les autorités préfectorales rappellent aux différentes collectivités territoriales leurs obligations légales concernant la création sur leurs sites Web d'un espace d'expression réservé aux groupes de l'opposition, sous réserve que ces sites puissent être analysés comme des bulletins présentant des bilans d'actions – ce qu'ils sont très souvent.

Orientation n° 8 : renforcer l'expression démocratique sur les sites Web des collectivités territoriales

Rappeler par circulaire aux maires et présidents des organes délibérants des collectivités territoriales leur obligation de réserver un espace d'expression aux élus de l'opposition sur les sites Web présentant les actions de ces collectivités.

(1) Cf. http://www.ville-nice.fr/Collectivites/Actualites/Tribune-de-l-opposition
(2) Cf. http://www.strasbourg.eu/vie-democratique/municipalite/tribune_expression

B. UN OUTIL DE DÉLIBÉRATION

Les nouvelles formes dites « collaboratives » d'Internet ont dégagé des perspectives de développement supplémentaires pour la *e-démocratie*. Internet ne facilite pas seulement la communication entre les élus et les citoyens ; il rend maintenant possible la participation directe de ces derniers à la gestion des affaires publiques en faisant des citoyens eux-mêmes des sources d'informations pour les prises de décisions.

Le recours aux moyens électroniques pour développer de nouvelles formes de gouvernance demeure encore peu développé en France. L'ONU, en 2010, a procédé à un classement qui place la France au dixième rang mondial en matière de *e-gouvernement* mais au quinzième pour la *e-participation* (1). Dans les deux types de classement les pays anglo-saxons sont mieux placés que notre pays.

Cet engagement des citoyens par le biais des communications numériques constitue une nouvelle dimension pour la vie démocratique qui peut prendre plusieurs formes et engendre des problèmes nouveaux.

1. Les pétitions électroniques

La modalité de participation citoyenne la plus simple consiste à recourir à Internet pour faire part, aux autorités compétentes, de souhaits et de doléances. La procédure ancienne consistant à présenter des pétitions trouve, dans le monde numérique, l'occasion de se rénover et d'acquérir une plus grande effectivité.

Plusieurs parlements ont mis en place une procédure de pétition électronique. Le Parlement européen a ainsi reçu, en 2009, 65 % de ses pétitions sous forme numérique et prévoit de créer un portail interactif. En Allemagne, où le droit de pétition est inscrit dans la loi fondamentale, un portail de dépôt de pétitions en ligne a été ouvert sur le site du *Bundestag* (2). Le parlement Écossais propose également le dépôt de pétitions en ligne par le biais d'une plateforme particulièrement riche en fonctionnalités (3).

En France, la réforme constitutionnelle de 2008 a renforcé la procédure de la pétition en permettant la saisine, par cette voie, du Conseil économique, social et environnemental (CESE) sur toute question relevant du champ de compétence de ce dernier. Les conditions formelles fixées par la loi organique du 28 juin 2010 sont les suivantes : « La pétition est rédigée en français et établie par écrit. Elle est présentée dans les mêmes termes par au moins 500 000 personnes majeures, de nationalité française ou résidant régulièrement en France. Elle indique le nom, le prénom et l'adresse de chaque pétitionnaire et est signée par lui. » (4)

---

(1) http://www2.unpan.org/egovkb/global_reports/10report.htm

(2) https://epetitionen.bundestag.de/index.php?PHPSESSID=46e3685173830fb200b9d101fff6373b&action=petition;sa=new

(3) http://epetitions.scottish.parliament.uk/default.asp#starting

(4) Art.5 de la loi organique n° 2010-704 du 28 juin 2010 relative au Conseil économique, social et environnemental.

Le législateur n'a pas précisé la nature du support matériel de la pétition. Il reviendra au Conseil économique, social et environnemental d'évaluer si le média Internet est susceptible de remplir les conditions légales de dépôt. Dans un rapport remis au Président de la République en 2009, M. Dominique-Jean Chertier privilégiait cette solution : « *L'optique du droit de pétition citoyen devant le CESE et l'opportunité d'en faciliter l'exercice plaident pour un dispositif essentiellement électronique (par ailleurs écologiquement irréprochable) […] Les signatures s'effectueraient à titre principal par le biais du site Internet du CESE qu'il conviendrait d'adapter à cette fin* » (1) Une telle voie ne pourra cependant être retenue que si des solutions techniques fiables sont trouvées pour parer les risques importants de fraude, qu'il s'agisse de l'envoi en masse de pétitions par automatisation ou de falsification des signatures.

2. Les nouveaux moyens d'expression et de débat en ligne

De nombreux élus ont créé sur Internet des comptes personnels sur lesquels les administrés les informent en continu des problèmes qu'ils rencontrent ; selon M. Marc-Antoine Jamet (2), représentant de l'association des maires de France, les administrés préfèrent maintenant s'adresser directement à leur maire plutôt qu'aux services de leur mairie. L'élu est ainsi assailli de demandes pour lesquelles une réponse est exigée très rapidement ; une telle urgence n'est pas toujours compatible avec la nécessité de fournir des renseignements de qualité.

Ce constat relève une des difficultés de l'utilisation d'Internet : en facilitant la communication, ce média multiplie les sources de participation et suscite la production d'un très grand nombre d'informations disparates. Pour que les informations produites par les citoyens gardent leur utilité, et que la *e-démocratie* ne soit pas un leurre sous la forme d'espaces d'expression déliés de la réalité des affaires publiques, il convient de mettre en place des procédures de classement et de suivi des informations.

Une des formes les plus effectives de participation citoyenne par le biais d'Internet consiste à signaler un dysfonctionnement dans certains aspects de la gestion des services publics. Les sites anglo-saxons sont en ce sens exemplaires par le pragmatisme dont ont fait preuve leurs concepteurs. Le site *Fixmystreet,* (3) au Royaume-Uni, permet, par exemple, d'indiquer avec précision sur une carte un lieu qui demanderait l'intervention des services d'entretien de la voirie. Chaque message peut être lu par l'ensemble des internautes ainsi que la réponse que les services ont apportée à la demande. Le système rend possible la visualisation sur la carte de la ville de tous les signalements ; une vue d'ensemble des problèmes d'entretien est donc constamment offerte.

---

(1) Pour une réforme du Conseil économique, social et environnemental*, rapport au Président de la République, 15 janvier 2009, La Documentation française.*

(2) Audition du 8 décembre 2010.

(3) Cf. http://www.fixmystreet.com/

Cette plateforme fait partie d'un ensemble d'actions citoyennes initiées par l'association *UK Citizens Online Democracy*. Dans ce cadre, ont été également lancés un site sur lequel les internautes peuvent interroger leurs représentants au Parlement, un site de pétitions et un site d'appel à projet pour des actions de bénévolat.

On trouve peu d'initiatives équivalentes en France qui proposeraient une plateforme pérenne sur laquelle les citoyens pourraient soumettre leurs observations et propositions sur un ensemble de thématiques. (1)

Les outils de débats en ligne mis en place sur les sites français voient leurs usages orientés principalement vers le traitement de projets ponctuels, relatifs notamment à l'aménagement du territoire. Comme l'a souligné M. Olivier Devillers, chargé de mission au sein de l'association des maires des grandes villes de France, *« aucun sujet n'échappe à un débat sur Internet, surtout s'il s'agit d'un " sujet qui fâche ".* »(2)

Les réactions des administrés sont recueillies par le biais de blogs et de forums de discussion.

Des formes encore plus sophistiquées de participation sont proposées par certaines municipalités. Ainsi, à Rennes, des « *Web meetups* » ont été organisés autour d'un projet d'aménagement : il s'agissait de proposer des visites virtuelles de futurs aménagements urbains ; les visiteurs avaient la possibilité de se communiquer entre eux leurs remarques sur le projet présenté en trois dimensions et à l'intérieur duquel ils pouvaient faire se déplacer un personnage virtuel les représentant. (3).

À Paris, la Charte parisienne de la participation, dans son édition 2010, a prévu de développer la « *e-participation* » et d'ouvrir une rubrique spécifique sur le site officiel de la Mairie de Paris qui permettra « *de faire connaître toutes les remarques et suggestions sur un projet.* » Il est également proposé de favoriser « *l'expression citoyenne directe et les débats participatifs* » en recourant à de nouveaux supports : « *appel à propositions et système de votes commentés en ligne ; contributions collectives de type « wiki » ; interface de pétitions citoyennes en ligne.* » Par ailleurs, la Charte précise que tous les documents relatifs à un processus participatif doivent être accessibles en ligne.

Le recours à Internet dans le but de recueillir les avis des personnes intéressées peut se faire à une échelle plus large. Ainsi, considérant que les meilleurs juges des complexités excessives des normes juridiques sont les citoyens eux-mêmes, M. Jean-Luc Warsmann, président de la commission des Lois de l'Assemblée nationale et de la présente mission, a été à l'initiative de l'ouverture,

---

(1) Un site intitulé « Ma mairie citoyenne *» a été créé en novembre 2010. Il permet aux personnes intéressées de lancer des débats sur un sujet concernant son territoire. Cf :http://www.mamairie-citoyenne.fr/*

(2) Audition du 8 décembre 2010.

(3) Cf. http://www.innovcity.fr/2010/05/25/rennes-experimente-un-outil-de-mediation-citoyen-pour-un-projet-d%E2%80%99amenagement/

en septembre 2007, d'un portail d'accueil sur le site Internet de l'Assemblée nationale sur lequel pouvaient être formulées des suggestions de simplification. Plus de 500 contributions ont été recueillies et mises en ligne en un an ; cette procédure a conduit au dépôt, par le président Jean-Luc Warsmann, de près de 30 questions écrites et à l'adoption de dispositions législatives visant à simplifier le droit.

La simplification du droit et des procédures administratives fait également l'objet d'un débat interactif sur le site de la direction générale de la modernisation de l'État (DGME). Depuis le lancement, en juin 2009, du site *ensemble-simplifions.fr*, les administrés ont proposé près de 500 pistes de simplification qui ont été soumises aux votes et commentaires des internautes ; plus de 4 000 votes ont été recensés et 700 commentaires ont été envoyés. Les pistes les plus plébiscitées ont été étudiées par la DGME pour venir alimenter le programme des « *100 simplifications* » des démarches administratives lancé par le conseil de modernisation des politiques publiques et suivi dans le cadre de la révision générale des politiques publiques. Aujourd'hui, sur les 50 mesures qui composent d'ores et déjà ce programme, un tiers (17) sont issues du site *ensemble-simplifions.fr* (1).

3. L'expérience acquise par la commission nationale du débat public

Aussi développés que soient ces processus participatifs, il reste à savoir s'ils constituent l'amorce de débats ou s'ils demeurent, sous une forme certes plus interactive, de simples outils d'information au moyen desquels les institutions prennent connaissance des avis des citoyens. Des instruments destinés à animer un débat doivent en effet être aptes à mettre en avant des désaccords ou à susciter des consensus dans le but de prendre des décisions.

La mission d'information a donc interrogé la Commission nationale du débat public (CNDP) qui a la charge d'organiser des débats dont les résultats ne sont pas seulement des éléments d'information pour les maîtres d'ouvrage mais représentent pour ces derniers une contrainte dans le processus de décision ; en effet, le maître d'ouvrage est obligé d'indiquer les mesures qu'il juge nécessaire de mettre en place pour répondre aux enseignements qu'il tire du débat public (2). Pour autant, le débat n'est pas une instance de décision car il conduit à formuler un avis. La CNDP lance ainsi des consultations qui sont plus que des recueils d'informations mais moins que des instances de décision. Plus de 60 débats publics ont été tenus depuis 2002, date de la transformation de la CNDP en autorité administrative indépendante. On citera, parmi les grands débats récents, celui organisé à la demande de plusieurs ministères sur les options générales en matière de développement et de régulation des nanotechnologies, clôturé en

(1) Source : réponse au questionnaire adressé à la DGME par les rapporteurs de la mission.
(2) Cf. article L. 121-13 du code de l'environnement.

février 2010, et celui qui a porté sur le projet de réseau de transport du Grand Paris, achevé en janvier 2011.

L'utilisation d'Internet est systématique dans le cadre de ces procédures. Un site Internet est créé pour chaque débat public ; y sont accessibles en ligne les retransmissions des réunions publiques ainsi que les documents relatifs au projet soumis à discussion. Le site sert de plateforme où les internautes peuvent poser des questions aux maîtres d'ouvrage, déposer des contributions et formuler des propositions sous forme de « cahiers d'acteur ». Pendant la tenue des réunions publiques, des questions en ligne peuvent être posées en direct.

La mission d'information s'est interrogée sur la façon dont, dans ce type de débat, on pouvait s'assurer de l'identité des intervenants sur Internet et de leur intérêt réel pour le sujet débattu. De même, a été soulevé le risque que des représentants d'une position très minoritaire ne s'emparent de cet outil pour s'exprimer massivement, par le jeu de fausses identités, et ne détournent à leur profit l'ensemble de la consultation. Cette menace semble en effet peser sur tout type de débat organisé sur Internet.

Mais comme l'a expliqué M. Philippe Marzolf, vice-président de la CNDP [(1)], la réussite des débats dont la CNDP a la responsabilité est conditionnée par les limites mêmes de la procédure. Il ne s'agit pas, en effet, de prendre une décision sur l'avenir du projet discuté mais de recueillir divers arguments auxquels devront répondre les maîtres d'ouvrage. Ainsi la question de l'identité réelle des intervenants ne se pose pas. De même, d'éventuels détournements de procédure n'ont pas d'effet sur le résultat de la consultation, la valeur d'une position ne tenant pas au nombre de personnes qui la défendent mais à la pertinence des arguments qui la soutiennent.

La préoccupation des organisateurs des débats de ne faire émerger que le contenu rationnel des diverses opinions conduit à une utilisation d'Internet quelque peu à rebours des pratiques en vogue. Ainsi, la CNDP a dû mettre fin à l'expérience qu'elle avait lancée consistant à créer, sur le site Internet de chaque débat, des forums de discussions car la vigueur des propos qui y étaient tenus rendait difficile la modération des messages reçus.

Si les instruments de débat en ligne proposés par la CNDP peuvent ainsi apparaître relativement figés au regard de la souplesse et de la convivialité d'autres sites, cela résulte d'un choix répondant aux exigences d'une mission. Les contraintes de forme imposées aux interventions des internautes conduisent d'ailleurs à la formulation de critiques mieux articulées et mieux fondées que les propos, toujours plus tranchants et polémiques, tenus dans le vif des réunions publiques.

Le bilan tiré par les responsables de la CNDP de l'utilisation des outils numériques est donc contrasté. La complexité des sujets abordés et la portée des

(1) Audition du 8 décembre 2010.

décisions à prendre conduisent à écarter le recours à certains instruments de communication. Autrement dit, tous les outils de communication proposés sur le marché du Web collaboratif ne font pas de bons moyens de réflexion et de décision.

D'autres difficultés sont par ailleurs connues. Le risque existe de créer de faux débats sur Internet, soit en recrutant des équipes de rédacteurs faisant artificiellement vivre un site, soit en passant sur des réseaux sociaux pour en exploiter l'aspect communautaire. Dans ce dernier cas, sont de fait exclus les internautes qui ne souhaitent pas être membres d'un réseau. Construire un débat autour de communautés « d'amis » dans l'espoir de disposer d'intervenants motivés reviendrait à restreindre la participation à des profils d'individus spécifiques et à battre en brèche la notion même de publicité de la discussion.

L'argument peut aussi être retourné selon lequel Internet propose un lieu de débat apaisé alors que l'organisation de débats « physiques » suscite parfois des confrontations extrêmement vives. Quelle juste mesure trouver entre la volonté de sauver un débat en l'organisant sur Internet parce qu'il ne peut plus se tenir physiquement en raison de l'opposition déterminée de certains participants, comme il en a été du débat sur les nanotechnologies, et le risque de substituer au débat réel devant des personnes physiques, des débats virtuels, sans interlocuteurs visibles et ne rendant pas compte clairement des oppositions ni des clivages qui traversent la société ?

4. Les questions de méthode posées par les débats sur Internet

Pour ne pas tomber dans la thèse extrême, défendue par certains, qui pourrait se profiler derrière certaines de ces critiques et qui consisterait à dire que la structure même d'Internet est plus un obstacle à la réflexion et à la démocratie éclairée qu'un progrès des Lumières, il conviendrait de disposer d'analyses, ou au moins de retours d'expérience, sur l'effectivité et les méthodes des différentes formes de débats publics. Cet aspect méthodologique apparaît essentiel pour donner un avenir à la *e-démocratie*.

Les acteurs engagés sur ces questions ont d'ailleurs parfaitement mesuré la portée de cet enjeu. Au niveau européen, la recommandation aux États membres du Conseil de l'Europe, adoptée le 18 février 2009, demande que soient évalués les méthodes et outils de la démocratie électronique « *sur les plans qualitatif et quantitatif, si possible, par une tierce partie. L'évaluation devrait porter sur leurs qualités en termes de démocratie, de gouvernance, de participation publique et de démocratie électronique, sur leur convivialité, leur acceptabilité et leur degré effectif d'acceptation* ». (1)

(1) Recommandation CM/Rec (2009)1 du Comité des ministres aux États membres sur la démocratie électronique, adoptée par le Comité des Ministres le 18 février 2009.

Au plan local, la Charte parisienne de la participation, précédemment citée, consacre sa « neuvième clef » à la mise en œuvre d'actions de formation portant sur la pratique de la concertation et de la participation.

Sur ces questions de méthodologie, la mission d'information regrette que la CNDP ne partage pas mieux la riche expérience qui est la sienne. L'article L. 121-1 du code de l'environnement lui donne pourtant la mission « *d'émettre tous avis et recommandations à caractère général ou méthodologique de nature à favoriser et développer la concertation avec le public* ». La portée de cette disposition semble cependant réduite dans son application ; aux demandes d'avis dont elle est saisie, la CNDP répond en nommant une personnalité indépendante garantissant la mise en œuvre de la concertation. Même si la CNDP a pour seule mission le recueil des arguments et ne pourrait prétendre pouvoir rendre compte d'un processus démocratique mené à son terme, il serait des plus utiles – cette première étape de synthèse des arguments conditionnant toutes les autres – que les bilans d'expérience soient partagés et que des recommandations soient formulées. Les diverses institutions publiques, tant au niveau national que local, amenées à lancer des débats publics, verraient leurs procédures mieux assurées si elles pouvaient disposer d'un cadre méthodologique mieux défini. Si la notion de démocratie numérique doit avoir un avenir, il est nécessaire de garantir au citoyen internaute que les débats auxquels les institutions l'invitent sur le Net ne sont pas, en leur nature même, des débats tronqués.

Orientation n° 9 : rendre plus transparentes les procédures d'organisation des débats publics sur Internet

Garantir à chaque citoyen participant à un débat public par le biais d'Internet la transparence des règles selon lesquelles sa participation est prise en compte. À cette fin, formuler des recommandations sur l'organisation de ces débats, leurs méthodes, leurs audits, la formation des organisateurs, lesquelles pourraient servir de référentiel pour les initiatives de *e*-démocratie prises par les institutions publiques. Cette mission pourrait revenir à la Commission nationale du débat public dans le cadre des compétences qui lui sont déjà reconnues.

C. LE VOTE ÉLECTRONIQUE : INTERNET PEUT-IL ÊTRE UN INSTRUMENT DE DÉCISION POLITIQUE ?

Dès le moment où Internet est devenu un média de communication grand public, la question de son utilisation comme instrument de l'expression de la volonté des citoyens, à savoir comme moyen de vote, s'est posée.

a) Les avantages escomptés

Toutes les techniques de vote électronique ne recourent pas à Internet. Il en va ainsi des machines à voter ou des réseaux locaux de postes informatiques installés sur les lieux de vote. Mais l'utilisation d'Internet mettrait à profit les nombreuses possibilités du monde numérique ; c'est pourquoi, la mission

d'information s'est interrogée sur les avantages et les limites d'une procédure de vote qui passerait par le biais du Web.

En une première approche, le recours au vote électronique paraît offrir de nombreuses facilités : disposer d'une procédure qui évite la contrainte de se déplacer sur les lieux de vote, supprimer les fastidieuses opérations de dépouillement des bulletins, encourager la démocratie directe, lutter contre l'abstention, faciliter le vote des personnes handicapées et celui des citoyens expatriés.

Pour tous ces motifs, le Conseil de l'Europe encourage le développement de cette technique. Souhaitant renforcer la participation des citoyens aux processus politiques, le Conseil a adopté le 30 septembre 2004 une recommandation portant sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (1). Les 16 et 17 novembre 2010, la troisième réunion biennale du Conseil de l'Europe organisée en vue d'examiner les évolutions dans le domaine du vote électronique a été l'occasion de confirmer les orientations prises en 2004 (2). Cette position s'est surtout appuyée sur le bilan des quatre élections organisées en Estonie, de 2005 à 2009, qui ont été les premières à expérimenter à grande échelle cette procédure.

En France, quelques procédures de vote électronique à distance ont été autorisées : en 2001, pour les actionnaires de sociétés anonymes lors des assemblées générales (3) ; en 2003, pour l'élection des membres de l'Assemblée des Français de l'étranger par les Français inscrits sur les listes électorales consulaires (4) ; en 2004, pour l'élection des délégués du personnel ou des délégués au comité d'entreprise, sous réserve de la conclusion d'un accord d'entreprise (5) ; en 2007, sur le fondement d'une ordonnance de 2004, pour l'élection à Paris des conseillers prud'hommes du 3 décembre 2008 (6) ; en 2009, pour l'élection des députés par les Français établis hors de France (7) et enfin en 2010, pour les élections des membres des conseils des établissements publics à caractère culturel, scientifique et professionnel (8).

(1) Rec (2004) 11 du 30 septembre 2004.

(2) L'ensemble des documents présentés au cours de cette réunion est accessible sur le site : http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/default_FR.asp.

(3) Décret n° 2002-803 du 3 mai 2002 portant application de la troisième partie de la loi n° 2001-420 du 15 mai 2001 relative aux nouvelles régulations économiques.

(4) Loi n°2003-277 du 28 mars 2003 tendant à autoriser le vote par correspondance électronique des Français établis hors de France pour les élections de l'Assemblée des Français de l'étranger.

(5) Art. 54 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

(6) Ordonnance n° 2004-603 du 24 juin 2004 et décret n° 2007-1130 du 23 juillet 2007.

(7) Ordonnance n° 2009-936 du 29 juillet 2009 relative à l'élection de députés par les Français établis hors de France.

(8) Loi n° 2010-500 du 18 mai 2010 tendant à permettre le recours au vote par voie électronique lors des élections des membres de conseils des établissements publics à caractère scientifique, culturel et professionnel.

b) Les obstacles

Le législateur français est malgré tout resté prudent face à une technique dont on peut se demander si elle offre des garanties suffisantes au regard des principes fondant la validité de toute opération électorale.

Des questions se posent en effet à toutes les étapes du processus de vote.

Le processus de comptage des voix n'étant pas concrètement observable, les principes de sincérité et de surveillance effective des opérations de vote peuvent difficilement être invoqués.

À l'occasion du bilan de l'élection présidentielle de 2007, le Conseil constitutionnel a évoqué cet aspect à propos des machines à voter :

« L'usage de l'urne et des bulletins, le dépouillement manuel rendent palpables et familières les opérations électorales. Un contrôle mutuel, visuel, est rendu possible par la présence physique des scrutateurs. La participation aux opérations qui se déroulent dans un bureau de vote associe les citoyens à une sorte de liturgie républicaine.

L'intrusion des machines à voter dépossède les citoyens de tout cela. Elle rend opaque ce qui était visible. Elle met fin à une « communion citoyenne ». Elle prive le corps électoral de la surveillance collective des opérations dans lesquelles s'incarne le suffrage universel. Elle rompt le lien symbolique noué par la pratique « manuelle » du vote et du dépouillement. » (1)

Le Conseil constitutionnel explique les réactions de rejet des machines à voter par des causes plus psychologiques que techniques, l'agrément dont bénéficient ces appareils devant suffire, selon les juges, pour en garantir le bon fonctionnement.

Il est évident que la question est plus complexe encore dans le cas d'une procédure de vote par le biais d'Internet. Les incertitudes relatives à la sécurité des transmissions de données sur le Net sont en effet plus nombreuses que pour des systèmes fonctionnant en boucle locale.

Ainsi, à l'occasion d'un incident informatique intervenu au cours des élections prud'homales à Paris, en novembre 2008, la CGT s'était plainte, dans une lettre au ministre du Travail, de l'opacité de la procédure du fait de sa technicité : « *Compte tenu du caractère complexe de ces interventions, nos déléguées ont pu observer que seuls des experts informatiques avaient la maîtrise de toutes les opérations effectuées*. […] *En l'état, les déléguées de liste de la CGT ne peuvent attester de la sincérité du scrutin*. » (2) La CGT a formulé les mêmes inquiétudes pour les élections professionnelles auxquelles participeront les agents

(1) Bilan synthétique des deux tours de l'élection présidentielle de 2007.
(2) Communiqué du 27 novembre 2008 : http://www.cgt.fr/spip.php?article35385.

du ministère de l'éducation nationale le 20 octobre 2011 et pour lesquelles est prévu un recours exclusif au vote électronique.

Par ailleurs, nul contrôle ne peut être exercé sur les conditions dans lesquelles l'internaute vote depuis son ordinateur. Notre collègue Charles de La Verpillière, dans son rapport rédigé au nom de la commission de Lois sur le projet de loi ratifiant l'ordonnance relative à l'élection des députés par les Français établis hors de France, avait ainsi eu l'occasion de citer les réserves formulées par le Conseil d'État sur le projet d'ordonnance : « *les précautions prises par le pouvoir réglementaire afin d'assurer la fiabilité technique des opérations par voie électronique et garantir l'anonymat des suffrages ainsi émis ne sauraient, en effet, prémunir l'électeur contre l'indiscrétion ou les pressions de son entourage lors de l'accomplissement de son vote.* » (1) Cette procédure garantit difficilement le caractère secret, personnel et libre du scrutin.

On ne peut pas non plus écarter le risque que le secret du vote soit levé par le biais d'une identification de l'adresse du poste informatique utilisé. Le sens même du vote risquerait d'être modifié en cas de piratage.

Le Conseil de l'Europe encourage cette procédure de vote, estimant qu'elle constitue un moyen efficace pour renforcer la participation des citoyens aux processus démocratiques. La consultation des documents publiés par les experts à l'occasion de la troisième réunion biennale, organisée en novembre 2010, en vue d'examiner les évolutions intervenues dans le domaine du vote électronique met pourtant bien en évidence les nombreuses difficultés techniques qui restent à surmonter. Il y est ainsi souligné que le vote électronique exige une sécurisation des procédures beaucoup plus stricte que le vote traditionnel par bulletin papier. « *Un média électronique exige de fortes protections contre les mésusages. Des « firewall » doivent être élevés, les votes doivent faire l'objet d'un cryptage et d'un décryptage, tous les types de cyber attaques doivent être pris en considération. Il est important qu'à tous les niveaux soit mis en place un système de protection robuste. Le but principal d'un système sécurisé est d'avoir un système qui garantisse à chaque citoyen inscrit sur les listes de pouvoir voter et que son vote soit exactement pris en compte à la clôture du scrutin.* » (2). La nécessité de sécuriser les serveurs utilisés et les difficultés que posent les votes passant par des serveurs localisés à l'étranger sont également évoquées (3). Même si le bulletin est crypté, les possibilités qu'il soit détruit par

(1) Cf. Rapport n° 3026, 8 décembre 2010, de M. Charles de La Verpillière, ratifiant l'ordonnance n° 2009-936 du 29 juillet 2009 relative à l'élection de députés par les Français établis hors de France (n° 1894), p. 84 et Conseil d'État, Rapport public 2010*, p. 148.*

(2) Manuel sur le vote électronique – Étapes clés dans la mise en œuvre des élections par voie électronique, Conseil de l'Europe, novembre 2010, p.31.
http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/default_FR.asp

(3) La CNIL avait fait part des mêmes préoccupations pour les élections prud'homales de 2008. Cf. délibération 2006-237.

une cyber attaque, que le serveur de réception soit l'objet d'un dévoiement [1] ou d'un déni de service [2] doivent être envisagées.

La CNIL a formulé, le 21 octobre 2010 [3], plusieurs préconisations portant sur la sécurité des systèmes de vote électronique. Elle a recommandé, en particulier, la mise en place d'une expertise indépendante des systèmes de vote électronique et le recours à des techniques de chiffrement réputés « *forts* » de toutes les liaisons utilisées conformément au Référentiel général de sécurité [4].

Une expérience de vote électronique à une échelle encore jamais atteinte sera possible pour les prochaines élections des députés élus par des Français établis hors de France. La disposition légale qui le permet rappelle cependant que celle-ci devra se faire *« au moyen de matériels et de logiciels permettant de respecter le secret du vote et la sincérité du scrutin »* [5]. Après la ratification de l'ordonnance qui a introduit cette procédure, un décret en Conseil d'État devra en déterminer par décret les conditions d'application.

Malgré les risques potentiels que présente le vote par Internet, il est certain que les difficultés rencontrées par les Français de l'étranger pour se rendre dans les bureaux de vote et les problèmes d'acheminement des votes par correspondance font d'Internet un outil extrêmement utile susceptible de lever des obstacles insurmontables pour nombre de nos compatriotes. Cependant, ce n'est qu'au regard d'une mise en balance des avantages et des risques que la procédure électronique paraît, en l'état de la technique, acceptable.

Il apparaît finalement que les procédures de vote sur Internet peuvent présenter un intérêt et être encouragées si elles n'ont d'autre but que de recueillir des opinions dans le cadre d'enquêtes ou de mouvements d'opinion. Dans ce cas, il s'agit d'un moyen souple de communication qui permet de mesurer des engagements ou des préférences. Mais transformer ce moyen d'expression en un outil de décision serait méconnaître la fragilité intrinsèque du Web, lieu de tous les détournements. On peut même craindre que réussir à fausser un vote politique d'importance ne stimule la communauté des pirates informatiques.

Orientation n° 10 : **mieux mesurer les risques de détournement que présentent les procédures de vote par Internet**

Engager une évaluation indépendante et transparente des procédures de vote par le biais d'Internet.

*

* *

(1) Ou « pharming » : technique de piratage qui redirige l'internaute vers un site frauduleux.
(2) Technique de piratage consistant à rendre indisponible un service.
(3) Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.
(4) Cf. partie V du présent rapport.
(5) Article L. 330-13 du code électoral.

Si l'analyse de l'importance prise par Internet pour les individus conduit à réfléchir à de nouvelles exigences en matière de droit de communication et à des formes renouvelées d'engagement politique, elle amène naturellement à s'interroger sur le rôle pris par Internet pour l'institution représentant la collectivité des individus, à savoir l'État. Quels profits l'individu peut-il attendre d'un recours massif à l'outil numérique de la part des organismes d'État ? Mais quelles garanties nouvelles l'individu est-il, aussi, en droit de revendiquer pour que les politiques de modernisation de l'État, fondées sur des instruments de gestion de données d'une redoutable efficacité, ne débouchent pas sur des atteintes à ses droits propres ?

TROISIÈME PARTIE : INTERNET, DE NOUVEAUX RAPPORTS ENTRE LES CITOYENS ET L'ÉTAT

I. LA *E*-ADMINISTRATION

Si l'émergence des nouveaux outils numériques a fait évoluer la façon dont les citoyens s'impliquent dans l'activité politique, sans pour autant que l'on puisse dire que le socle des valeurs démocratiques en ait été modifié, Internet semble bien avoir révolutionné le rapport de l'individu et de l'État en tant que gestionnaire des affaires publiques. En quelques années, la *e-administration* s'est développée dans toutes les sphères des services d'intérêt général. En rendant possible, 24 heures sur 24, l'accomplissement de démarches administratives sans que l'intéressé ait à se déplacer, en permettant des procédures simplifiées et regroupées et en rendant les normes juridiques plus accessibles, Internet contribue, peut-on penser, à inverser ce mouvement de bureaucratisation, de complexification et de distanciation par rapport aux administrés qui semblait jusqu'à présent caractériser l'État moderne.

Mais Internet ne peut être utilisé pour remodeler à ce point l'action de l'État sans qu'une approche politique claire de son utilisation ne soit formulée. C'est à cette condition qu'on tirera parti de toutes ses potentialités tout en excluant les mauvais usages auxquels pourrait incliner un outil de gestion si novateur.

A. UNE RÉVOLUTION DES PRATIQUES DE L'ADMINISTRATION

Le développement des médias numériques dans l'administration répond à deux objectifs : simplifier les rapports entre le citoyen et l'administration, et réaliser des économies de coût.

L'objectif de simplification porte tant sur le contenu des procédures que sur l'accès aux services administratifs. Il est en effet vite apparu que le recours à Internet ne devait pas se réduire à créer pour chaque administration un site Web sur lequel chaque secteur administratif rendrait disponibles les divers documents gérés dans son champ de compétence et proposerait, en format numérique, les formulaires papier déjà existants. La mise en place de services administratifs en ligne institue des rapports simplifiés avec les administrés qui ne supposent plus de leur part une connaissance *a priori* du découpage complexe des départements administratifs.

À cette fin, les capacités de partage en réseau sont mises à profit pour décloisonner les services de l'administration. La révolution numérique a d'abord lieu entre les administrations pour pouvoir se faire ensuite entre elles et les administrés et réaliser l'objectif de rendre accessible l'ensemble des services à partir d'un nombre réduit de sites Internet.

La prise en compte des économies de gestion susceptibles d'être engendrées par le passage à la *e-administration* a contribué aux efforts de mise en réseau. L'automatisation des processus, l'accès partagé aux documents et la souplesse introduite dans l'organisation des services du fait de la levée des contraintes liées à l'accès physique aux documents, sont en effet des facteurs de réévaluation des coûts liés à la réduction du nombre de documents papier mais surtout à une nouvelle affectation des moyens humains.

L'administré, accoutumé à l'environnement numérique, attend de l'administration des sites ergonomiques, des temps de réponse rapides et des informations riches et à jour. Mais surtout il exige que lui soit garanti un environnement de communication dans lequel il puisse avoir confiance car les données qu'il est amené à transmettre relèvent le plus souvent de la sphère privée.

1. Les plans successifs de modernisation

Le passage au numérique de l'administration française a eu pour préalable l'adoption de plusieurs dispositions législatives.

L'ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités a permis l'usage du support électronique comme moyen de communication et a validé le recours à la signature électronique. En matière civile, l'admission en preuve de l'écrit sous forme électronique avait été introduite dans le code civil, cinq ans auparavant par la loi du 13 mars 2000 (1).

Cette même ordonnance a par ailleurs imposé aux administrations le respect d'un référentiel de sécurité et d'un référentiel d'interopérabilité portant notamment sur les répertoires de données, les normes et les standards.

Plusieurs plans de dématérialisation des procédures administratives ont été conçus, dont les premiers ont précédé la mise en place des nouvelles dispositions légales.

• En 1998 a été lancé le programme d'action gouvernementale pour la société de l'information (PAGSI). Annoncé en août 1997 par le Premier ministre, M. Lionel Jospin, il y était prévu la généralisation des sites Internet publics et la mise en ligne des formulaires administratifs.

• Le plan RE/SO 2007 (2), présenté en 2002 par le Premier ministre, M. Jean-Pierre Raffarin, avait pour ambition de rendre la *e-administration* accessible à tous les Français à l'horizon 2007 et fixait en particulier pour objectif de faire de l'État un acteur de la société de l'information ayant vocation à

(1) La loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique a introduit la disposition suivante dans le code civil : Art. 1316-1 : « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. ».

(2) RE/SO : Pour une REpublique numérique dans la SOciété de l'information.

l'exemplarité. L'État devait pousser plus loin le recours au numérique en proposant non seulement le téléchargement des formulaires administratifs mais la dématérialisation des procédures.

• Le plan ADELE [(1)], plus spécifiquement consacré à l'administration électronique, a été engagé en 2004 et coordonné par une agence pour le développement de l'administration électronique.

• Le plan France numérique 2012, lancé en 2008, s'appuie sur l'engagement du traité de Lisbonne de développer l'administration électronique en Europe. Il formule un total de huit « actions » parmi lesquelles : la dématérialisation des échanges sans solution de continuité entre l'administration et les administrés, l'interopérabilité des administrations, l'archivage des documents dématérialisés et l'accessibilité des sites de l'administration [(2)].

• Le conseil de modernisation des politiques publiques a fixé, en juin 2010, de nouveaux objectifs à la réforme générale des politiques publique (RGPP) en matière d'administration en ligne. Parmi les mesures destinées à faciliter les rapports des administrés avec l'administration figure le développement des guichets uniques, notamment de la plateforme *mon.service-public.fr*. L'objectif est que « *toutes les démarches jugées prioritaires par les usagers, aujourd'hui réalisables à distance (par courrier), devront pouvoir l'être également en ligne d'ici à fin 2012.* » [(3)]

• En février 2011, M. François Baroin, ministre du Budget, des comptes publics, de la fonction publique et de la réforme de l'État, a précisé ce dernier objectif : fin 2011, l'État devra permettre aux usagers de réaliser 80 % de leurs démarches administratives en ligne.

• Enfin, au niveau européen, la Commission européenne a fait figurer en 2010 la *e-administration* parmi les actions du plan de stratégie numérique pour l'Europe. La Commission en appelle à la création de services en ligne administratifs transnationaux et met l'accent sur la nécessité de généraliser à l'ensemble de l'Europe les marchés publics électroniques [(4)].

2 Les réalisations

a) Les démarches administratives en ligne

La démarche administrative dématérialisée qui a connu, en France, le succès le plus rapide est la déclaration de revenus. Depuis 2006, le nombre de

(1) ADELE : ADministration ELEctronique.
(2) Cf. http://lesrapports.ladocumentationfrancaise.fr/BRP/084000664/0000.pdf.
(3) Cf. p. 5 du document de présentation de la RGPP, juin 2010. http://www.rgpp.modernisation.gouv.fr/fileadmin/user_upload/dossier_cmpp4.pdf.
(4) Une stratégie numérique pour l'Europe*, communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 26 août 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:FR:PDF.*

déclarations faites en ligne a doublé, atteignant le chiffre de 10,4 millions en 2010. En 2009, la procédure a été simplifiée : il n'est plus nécessaire de se procurer un certificat électronique auprès de la direction générale des impôts, ce qui permet de procéder à la télé-déclaration depuis tout poste informatique connecté à Internet.

Les services nationaux de *e-administration* sont aujourd'hui regroupés autour du site *service-public.fr.* dont l'opérateur est la direction de l'information légale et administrative (DILA) relevant des services du Premier ministre.

LES SITES *: SERVICE-PUBLIC.FR* ET *MON.SERVICE-PUBLIC.FR*

– service-public.fr :

Ce site reçoit cinq millions de visites par mois et propose les services en ligne suivants : changement d'adresse en ligne (qui concerne les 10 % de la population qui déménage chaque année) ; demande d'acte d'état civil (naissance, mariage ou décès) ; demande d'extrait du casier judiciaire (bulletin n° 3) ; demande en ligne de certificat de situation administrative (non-gage et non opposition) ; déclaration en ligne des revenus ; pré-demande de changement de titulaire de certificat d'immatriculation ; service de télépaiement des amendes ; des services en ligne pour les demandeurs d'emploi sont également proposés.

La mise en ligne des formulaires administratifs est régie par l'article 1er du décret n° 99-68 du 2 février 1999 qui dispose que : « *Les formulaires dont l'usage est nécessaire pour accomplir une démarche auprès d'une administration ou d'un établissement public administratif de l'État sont tenus gratuitement à la disposition du public, sous forme numérique, par le site public dénommé "service-public.fr".* » Ce dernier a mis 469 formulaires administratifs en ligne.

– mon.service-public.fr :

La création du service personnalisé « *mon.service-public.fr* » fait partie des initiatives les plus innovantes. Ce portail développé par la direction générale de la modernisation de l'État (DGME) est accessible depuis le site *service-public.fr*. En ouvrant un compte personnel, l'utilisateur a accès à un ensemble de services en ligne ; les démarches administratives proposées peuvent être réalisées intégralement à partir des données personnelles de l'utilisateur, les demandes pouvant être suivies à chacune de leur étape. Depuis l'ouverture du site, au début de l'année 2009, près de 1 700 000 comptes ont été créés sur ce portail. Le rythme d'ouverture de comptes s'accélère : on dénombre 300 000 nouveaux comptes depuis le début de l'année 2011.

Ce service offre treize prestations individualisées : déclaration de changement de coordonnées à l'attention de divers organismes ; demande d'inscription sur les listes électorales ; recensement citoyen obligatoire ; déclaration de changement de nom ; déclaration de perte et renouvellement de papiers ; services en ligne des allocations familiales ; services en ligne de l'assurance maladie ; chèque emploi service universel ; prestation d'accueil du jeune enfant ; services en ligne de l'assurance retraite (régime général de la sécurité sociale) ; services en ligne de la Mutualité sociale agricole ; déclaration de mini moto ou de mini quad ; services en ligne de la direction des retraites de la Caisse des dépôts.

En outre 17 formulaires administratifs peuvent être pré-remplis avec les informations du compte personnel. Les documents les plus demandés ont été les demandes de copie d'une décision de justice en matière civile, sociale ou commerciale ; les demandes de délivrance de certificat de non-pacte civil de solidarité et les demandes de certificat de non-appel.

Le neuvième rapport européen d'évaluation comparative sur l'administration en ligne a classé, au regard de son accessibilité, mon.service-public.fr au premier rang européen des guichets uniques, ex aequo avec Malte.

b) L'accès en ligne de toutes les normes juridiques françaises

Il revient à la DILA de mettre à disposition l'ensemble des normes juridiques françaises. Le site *Légifrance* rend accessible le *Journal officiel* électronique authentifié. Les textes qui y sont publiés sont opposables aux citoyens conformément à l'ordonnance n° 2004-164 du 20 février 2004 relative aux modalités et effets de la publication des lois et de certains actes administratifs. *Légifrance* rend accessible gratuitement l'ensemble des textes normatifs et les textes jurisprudentiels : Constitution, codes, lois, ordonnances et décrets ainsi que les arrêtés et les textes émanant des autorités administratives indépendantes. Les bulletins officiels des ministères y sont également publiés. Les textes de droit européen et international complètent ce corpus. Enfin, la jurisprudence y est accessible (Conseil constitutionnel, Tribunal des conflits, Conseil d'État, cours administratives d'appel et tribunaux administratifs, Cour de cassation, juridictions d'appel et juridictions du premier degré). Les conventions collectives sont également répertoriées.

c) Des services d'information administrative en ligne

La *e-administration* devant permettre aussi une communication allant dans le sens de l'usager vers l'administration, un service « Poser une question » est accessible depuis le site *Service-public.fr*. Le service garantit une réponse dans un délai de sept jours. Les questions sont posées par courriel, concernent les droits et les démarches des administrés mais doivent conserver un caractère général. En 2010, 78 507 courriels ont été traités(1).

La possibilité donnée aux citoyens de contacter directement un service a des conséquences importantes sur son fonctionnement et le bon accomplissement de sa mission. On peut ainsi mentionner l'élargissement, en 2009, des modes de saisine du Médiateur de la République rendu possible par Internet : « *le secteur Recevabilité a en effet mis en place un formulaire électronique. En quelques semaines, cet instrument a été plébiscité par les administrés qui, l'utilisant presque autant que le courrier classique, ont pratiquement fait doubler le nombre de demandes transmises au Médiateur de la République. Avantage : il permet d'accélérer les échanges lorsque le secteur a besoin d'informations complémentaires sur les réclamations, qui peuvent donc plus rapidement recevoir une réponse ou partir en instruction. Le succès de ce formulaire ne le destine néanmoins pas à se substituer au papier, les segments de population visés n'étant pas les mêmes*. » (2)

Le Médiateur peut par ailleurs être saisi de propositions de réforme administrative par le biais d'une plateforme informatique intitulée *Le Médiateur et Vous*. Les services de Médiateur répondent également en direct à des questions posées sous forme de « *chat* ».

---

(1) Source : service-public.fr, *chiffres et statistiques, http://www.service-public.fr/apropos-du-site/chiffres-statistiques/*

(2) Rapport annuel 2009*, p. 80.*

d) Vers une administration plus « collaborative »

Le développement de techniques permettant une implication croissante des internautes dans la production des informations disponibles sur le Net constitue une dimension de la *e-administration* rendue possible par le Web 2.0. Une administration moderne tournée vers l'usager doit en effet donner à ce dernier un rôle plus actif, en particulier dans l'évaluation des services qui lui sont proposés.

Le volet numérique du plan de relance lancé en 2008 a prévu de consacrer 20 millions d'euros à des projets de plateformes Web 2.0.

Comme il en a déjà été fait mention, la DGME a créé une plateforme interactive pérenne consacrée à la simplification de l'administration. Autour du slogan « *Vous contribuez, l'administration simplifie* » sont proposées trois formes de collaborations : déposer une proposition de simplification, donner son avis sur les propositions déjà en ligne et exprimer sa position sous la forme d'un vote. Quatre types de contributeurs ont été définis : les particuliers, les entreprises, les associations et les collectivités.

B. CRITIQUES ET AJUSTEMENTS

En dépit de nombreuses initiatives prises pour faire profiter les administrés des progrès du numérique, la révolution numérique a touché l'administration de l'État avec retard. Tel est le sentiment dont a fait part, devant la mission d'information, M. Arnaud Lacaze, chef du service « Projets » à la DGME [(1)]. Les comparaisons internationales ne sont pas non plus favorables à la France. Une étude comparative rendue publique par la Commission européenne le 21 février 2011 montre qu'en Europe, 80 % des démarches administratives de base peuvent être, en tout ou partie, réalisées par Internet [(2)]. Bien que la France atteigne un taux de 82 % de disponibilité, ce résultat ne la place qu'au 18e rang européen.

En février 2010, un groupe d'experts, dirigé par notre collègue Franck Riester, chargé d'analyser, à la demande du Gouvernement, la situation de l'administration numérique en France a mis en évidence plusieurs faiblesses du système actuel et formulé des suggestions d'amélioration [(3)]. L'offre de services n'est pas suffisamment organisée en fonction de l'usager. La terminologie utilisée sur les sites publics reste trop souvent très bureaucratique et l'avis de l'utilisateur sur le service rendu n'est pas sollicité. Prenant l'exemple des prises de rendez-vous en ligne, trop rarement proposées, et du recours insuffisant aux courriels pour répondre aux questions posées par les administrés, les auteurs de ce document estiment que toutes les fonctionnalités de base d'Internet ne sont pas généralisées

(1) Réunion du 14 décembre 2010.

(2) Neuvième rapport européen d'évaluation comparative sur l'administration en ligne.

(3) Amélioration de la relation numérique à l'usager, *rapport issu des travaux du groupe « Experts numériques », remis à M. Eric Woerth, ministre du Budget, des comptes publics, de la fonction publique et de la réforme de l'État et à Mme Nathalie Kosciusko-Morizet, secrétaire d'État chargée de la prospective et du développement de l'économie numérique (février 2010).*

et que le potentiel offert par le Net dans les échanges demeure sous-employé. Au niveau national, les sites présentent une hétérogénéité très forte tant dans leur présentation graphique que dans l'organisation interne de leurs données et services. Ce constat est encore plus marqué pour les sites des collectivités locales. Foisonnement – on compte plus de 400 sites d'État –, redondance, absence de visibilité et d'évaluation, absence de schéma directeur, non continuité de l'ensemble de la chaîne des services dématérialisés et manque d'accompagnement personnalisé constituent les défauts principaux de la *e-administration* française.

Parmi les suites données à ce rapport, il a été porté à la connaissance de la mission d'information la mise en œuvre d'un « schéma cible » discuté entre les ministères et dont l'objectif est de réduire à 60 le nombre de sites Web de l'État. Ce schéma a été validé lors du conseil de modernisation des politiques publiques du 30 juin 2010. L'introduction d'un référentiel général de qualité devrait contribuer à rendre plus homogène l'ensemble des plateformes proposant des services publics en ligne.

En matière de sécurité informatique, il est regrettable que le référentiel général de sécurité prévu par l'article 9 de l'ordonnance du 8 décembre 2005 précédemment mentionnée n'ait pu voir le jour qu'en 2010 [(1)] à l'issue d'un travail commun entre la direction générale de la modernisation de l'État et l'agence nationale de la sécurité des systèmes d'information.

Le Médiateur de la République a aussi invité les services publics, par le biais d'un communiqué de presse diffusé le 24 septembre 2010, « *à repenser l'utilisation des nouvelles technologies au sein des administrations pour que la dématérialisation n'aille pas de pair avec une déshumanisation du service public*. » Cette remarque avait été motivée par le constat d'un usage excessif des serveurs vocaux par certaines administrations.

Mais elle vaut aussi pour l'ensemble des mauvais usages faits des outils numériques par l'administration. Ainsi, les recommandations formulées par la charte *Marianne* pour améliorer l'accueil des administrés dans les services publics donnent, *a contrario*, quelques indications sur les progrès qu'il reste à réaliser en ce domaine : dans 8 cas sur 10 les courriels envoyés par les administrés aux services publics qui n'ont pas reçu le label de conformité au référentiel *Marianne* demeurent sans réponse. Seuls les 50 services qui ont été labellisés apportent la garantie de fournir, dans 85 % des cas, une réponse aux courriels en moins de 5 jours.

Il conviendrait de veiller à ce que certains outils de communication numérique ne se réduisent pas à des gadgets, ou pire encore, aggravent l'opacité des rapports avec l'administré. Les possibilités nouvelles de communication créent un rapport de confiance entre l'État et le citoyen ; ce dernier est persuadé que sa voix sera mieux entendue. Des garanties doivent être apportées pour éviter que

(1) Décret n° 2010-112 du 2 février 2010.

soient proposés des moyens de communication présentés comme devant répondre à cette attente mais ne procédant pas à un échange réel d'informations.

II. DES LIMITES DE LA MODERNISATION

A. IDENTITÉ ET CONFIDENTIALITÉ DES DONNÉES PERSONNELLES DES ADMINISTRÉS

Au regard de l'objectif de simplification qui sous-tend la dématérialisation des procédures administratives, la question s'est posée de savoir si cette mise en réseau des données devait modifier les exigences d'identification des administrés. Quel équilibre trouver entre le risque d'alourdir les procédures d'authentification en recourant à des outils censés faciliter les démarches administratives et celui de porter atteinte à la vie privée des administrés en employant des moyens numériques capables d'agréger de grandes masses de données et de les rendre facilement accessibles ?

M. Arnaud Lacaze, chef du service « Projets » au sein de la DGME, a expliqué devant la mission d'information [(1)] que, dans le cadre des téléprocédures, la vérification de l'identité des personnes se faisait selon deux principes. Le premier est **le principe d'équivalence** qui consiste à demander à l'utilisateur exactement le même document justificatif que celui exigé dans la procédure traditionnelle, seul le support de transmission étant modifié. Ainsi, les documents d'identité peuvent être scannés et envoyés par courriel à la mairie, ce qui équivaut à l'envoi par courrier d'une photocopie.

Le second est **le principe de proportionnalité** : les exigences en matière de contrôle des identités doivent être évaluées en fonction de leur nécessité. Il est, par exemple, évident qu'il convient de s'assurer au mieux de l'identité d'une personne bénéficiaire d'une prestation financière ; dans ce cas un certificat électronique est exigé. Dans les procédures de déclaration, l'utilisation d'un mot de passe et la fourniture de copies dématérialisées des documents exigés apparaissent suffisants, le même niveau de sécurité que celui exigé pour une démarche traditionnelle étant alors assuré.

Mais les données personnelles des administrés étant désormais hébergées sur des serveurs gérés sous la responsabilité des services administratifs, la *e-administration* ferait peser une menace sur les droits des individus si un niveau satisfaisant de sécurité des réseaux n'était pas assuré et si des contraintes juridiques fortes n'encadraient pas l'usage des données informatisées afin que des limites soient posées au pouvoir intégrateur des outils numériques.

(1) Audition du 14 décembre 2010.

1. Les risques liés à l'agrégation des données personnelles fournies à l'administration.

Les polémiques qu'avait suscitées le projet Safari (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus) lancé dans les années 1970 rappellent que les premières utilisations de l'informatique sont allées de pair avec l'ambition de croiser les informations sur les individus. Il s'agissait alors de relier les numéros Insee, nouvellement enregistrés sur un support informatique, avec ceux de la sécurité sociale, de la caisse nationale d'assurance vieillesse et des fichiers de la carte d'identité gérés par le ministère de l'Intérieur.

L'abandon de ce projet s'est fait dans un contexte de réévaluation des droits des individus face aux nouvelles technologies qui a conduit à l'adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Son article premier pose le principe suivant : « *L'informatique doit être au service de chaque citoyen. […]. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*. »

Concernant les fichiers de police, les députés ont eu l'occasion de débattre à plusieurs reprises de l'utilisation qui y est faite des données personnelles. En particulier, le fichier intitulé *Exploitation documentaire et valorisation de l'information générale* (EDVIGE) a fait l'objet, le 24 septembre 2008, d'un rapport d'information de M. Jean-Luc Warsmann, président de la commission des lois [(1)]. L'ensemble des fichiers de police a été abordé dans un rapport d'information présenté par nos collègues Mme Delphine Batho et M. Jacques Alain Bénisti [(2)]. Par ailleurs, ces deux députés sont en charge d'une mission sur la mise en œuvre des conclusions de leur rapport, en application de l'article 145-8 de notre Règlement ; c'est ce qui explique que la présente mission d'information n'a pas entendu traiter cette question spécifique.

Par ailleurs, deux projets récents visant à utiliser les outils numériques pour moderniser les services administratifs ont été l'occasion de rappeler les craintes suscitées par le projet Safari. Cependant, notre dispositif législatif permet aujourd'hui d'encadrer des utilisations de l'informatique qui, potentiellement, pourraient être susceptibles de dérives.

En 2009, la CNIL a été amenée à rendre un avis sur un projet de décret en Conseil d'État relatif au Répertoire national commun de la protection sociale (RNCPS), répertoire qui prévoyait l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR).

Le RNCPS contient des données d'identification des individus et des informations relatives à leur affiliation aux différents régimes et organismes pourvoyeurs de prestations. Ce dispositif sert de moyen de contrôle contre la fraude. Comme indiqué dans une réponse à une question écrite de M. Arnaud

(1) Rapport d'information n° 1126, 24 septembre 2008.
(2) Rapport d'information n° 1548, 24 mars 2009.

Richard, le dispositif « *vise à donner une photographie de la situation de chaque assuré afin d'éviter notamment que celui-ci ne touche des prestations incompatibles entre elles.* » (1)

Mais ne risquait-on pas de transformer la photographie d'une situation en une photographie d'identité ?

La CNIL a considéré que *« la création d'un nouveau traitement de données à caractère personnel d'ampleur nationale, comportant l'identité, le NIR, l'adresse et des données relatives à la nature des droits et prestations des bénéficiaires doit être assortie de garanties toutes particulières notamment en termes de sécurité et de confidentialité.* » (2).

Des garanties strictes semblent en effet avoir été apportées. Par exemple, les consultations du répertoire sont réservées à des fonctionnaires habilités et sont tracées ; le répertoire ne constitue pas en lui-même une base de données, celles-ci restant hébergées par les différents organismes consultés ; il ne produit en lui-même pas d'informations nouvelles et ne permet pas de modifier les données détenues par chaque organisme ; le répertoire est utilisé pour venir en complément d'examens réalisés au cas par cas ; la sécurité des échanges de données est assurée par un système de chiffrage ; enfin, les droits d'accès et de rectification peuvent s'exercer(3). Le RNCPS devrait être opérationnel à la fin de l'année 2011.

L'article 2 de la proposition de loi de simplification et d'amélioration de la qualité du droit (4) qui prévoit que « *les autorités administratives échangent entre elles toutes informations ou données strictement nécessaires pour traiter les demandes présentées par un usager* » a pu également susciter des interrogations.

Au cours des débats, notamment au Sénat, certains parlementaires se sont opposés au vote de ce texte estimant qu'il comportait le risque de permettre le croisement de données personnelles. Le précédent du projet Safari a d'ailleurs été rappelé à cette occasion (5). Au cours de son audition devant la mission d'information, M. Jean-Marc Manach, journaliste, a fait part des mêmes inquiétudes (6).

Cependant le texte en question a été rédigé par l'auteur de la proposition de loi, le président Jean-Luc Warsmann, précisément de telle façon que les garanties nécessaires soient apportées : l'échange de données est soumis à la législation relative à l'informatique, aux fichiers et aux libertés, les droits d'accès et de rectification sont garantis et la sécurité informatique exigée.

---

(1) Question n° 83426. Réponse JO *du 26 octobre 2010.*
(2) Délibération n° 2009-211 du 30 avril 2009 portant avis sur un projet de décret en Conseil d'État relatif au Répertoire national commun de la protection sociale (RNCPS).
(3) Décret n° 2009-1577 du 16 décembre 2009.
(4) Proposition de loi n°1890
(5) Cf. séance du 13 décembre 2010.
(6) Audition du 14 avril 2011.

Mais surtout, le dispositif est lié à la seule demande de l'administré et ne conduit à recueillir que les données strictement nécessaires à cet effet. Il n'a en rien une finalité de contrôle mais bien de simplification de la procédure dans l'intérêt de l'administré aux prises avec des administrations qui lui demandent plusieurs fois les mêmes informations pour traiter ses données. C'est l'usager du service public qui est à l'initiative de la demande, ce qui écarte le risque d'un échange de données qui interviendrait indépendamment d'une démarche expresse de sa part.

Il reviendra au Conseil d'État de prévoir de modalités d'application n'introduisant aucun risque de détournement, la CNIL devant par ailleurs, comme le précise le texte même de la proposition, rendre un avis motivé et publié sur les dispositions réglementaires qui seront prévues.

2. L'architecture originale du site *mon.service-public.fr*

Les mêmes inquiétudes auraient pu être suscitées par la création du site *mon.service-public.fr*.

La mise en réseau des services administratifs a relancé, en effet, l'idée d'attribuer un identifiant unique par l'intermédiaire duquel chaque administré pourrait accéder à toutes les données administratives le concernant. Le rapport précité de notre collègue Frank Riester a souligné combien « *la multiplicité des login et autres inscriptions préalables à l'utilisation d'un site sont préjudiciables* » (1) au regard de l'objectif de simplification des démarches.

Cependant, selon M. Perica Sucevic, conseiller juridique de la DGME - citant, lui aussi le précédent du projet Safari – un identifiant unique ne correspondrait pas « à la mentalité française », soucieuse des libertés individuelles.

Pour éviter cette difficulté, un système original a été mis en œuvre lors de l'élaboration du site *mon.service-public.fr* lancé le 19 octobre 2009 (2). L'utilisateur dispose d'un mot de passe lui donnant accès à une pluralité de comptes qui, tout en étant fédérés entre eux, conservent leur propre identité. L'accès au compte se fait donc à la seule initiative de l'administré, conformément aux exigences de la CNIL. L'administration ne peut pas avoir de regard transversal sur le contenu des comptes.

L'utilisation d'une technique de cryptage vise à rendre impossible pour un tiers l'agrégation, sous forme de base de données, des documents personnels placés par l'administré sur son espace de stockage. Comme le précise la fiche de présentation du site :

---

(1) Cf. rapport précité, p.21.

(2) La création de ce site résulte de l'article 7 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

« *L'usager maîtrise en toute circonstance les accès à cet espace confidentiel :*

– c'est lui qui autorise explicitement l'accès à ces données pour préremplir les formulaires administratifs en ligne ;

– c'est lui qui décide d'aller chercher une pièce justificative dans cet espace au cours d'une démarche en ligne ;

– c'est lui qui autorise un service en ligne à déposer le résultat d'une démarche en ligne (justificatif, attestation, récapitulatif, etc.) en vue de le stocker.

Aucune administration ne peut donc accéder à cet espace confidentiel à l'insu de l'usager, excepté dans le cadre d'une instruction judiciaire. » (1)

Il semblerait selon des informations fournies par la DGME, que le site n'ait pas fait l'objet d'attaques informatiques qui auraient mis en danger la confidentialité des données qui s'y trouvent.

3. La dématérialisation des actes authentiques et des pièces de procédure

L'encadrement réglementaire et les précautions techniques qu'exige le recours aux instruments numériques pour éviter tout mésusage au détriment des administrés ont également déterminé les conditions de déploiement des procédures de dématérialisation des actes authentiques.

La prudence à observer dans le développement des projets d'informatisation se traduit par un décalage important dans le temps entre le moment où l'autorisation législative ou réglementaire est donnée et celui où les outils informatiques sont effectivement utilisables. Il en va ainsi de la dématérialisation de l'acte authentique rendue possible par la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

L'écrit sous forme électronique a la même force probante que l'écrit sur support papier sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. Un acte authentique peut être dressé sur support électronique. (2)

Le décret en Conseil d'État précisant les conditions d'établissement et de conservation de ces actes n'est paru qu'en 2005 (3). La principale difficulté était de concevoir un système fiable et sécurisé. Il a ainsi fallu mettre à la disposition de chaque notaire des outils de signature sécurisée sous la forme de clés USB dont la

(1) https://mon.service-public.fr/portail/faces/jsp/nonauthent/securite.jsp
(2) Cf. articles 1316-1, 1316-3 et 1317 du code civil.
(3) Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires.

technologie a été certifiée par la direction centrale de sécurité des systèmes d'information le 12 septembre 2007. Un minutier central électronique accessible par un réseau intranet a été créé. La signature du premier acte authentique sur support électronique est intervenue le 28 octobre 2008. Au premier trimestre 2011, le dispositif reste de dimension modeste puisque le minutier n'a au total enregistré depuis sa création que 900 actes électroniques. Le nombre d'offices notariaux munis des outils numériques nécessaires devrait cependant augmenter au cours du second semestre 2011.

Le 1er octobre 2010 a été signé le premier acte authentique dans les tribunaux. Cette procédure dématérialisée est intégrée au système informatique d'application des décisions de justice « Minos » et est expérimentée dans les tribunaux de police de Bourges et de Bordeaux. Là aussi, les précautions de sécurité expliquent la lenteur du déploiement de cette technique.

Les techniques de numérisation ont aussi permis d'apporter une solution au problème ancien de l'accès aux pièces de procédure des dossiers d'instruction. Le décret n° 2007-1620 du 15 novembre 2007, pris en application de la loi n° 2007-291 du 5 mars 2007 renforçant l'équilibre de la procédure pénale, a autorisé la copie des pièces sous forme numérisée et leur envoi à l'adresse électronique de l'avocat. Ce dernier peut à son tour formuler des demandes d'acte à l'adresse électronique de la juridiction (1) sous réserve de l'existence de protocoles entre les barreaux et les juridictions. La nécessité de garantir la sécurité des échanges d'information auxquels il est procédé dans ce cadre a conduit à la création du réseau sécurisé RPVA – réseau privé virtuel avocats – validé par une convention signée le 28 septembre 2007 par le ministre de la Justice et le président du Conseil national des barreaux.

B. L'ÉGALITÉ DES ADMINISTRÉS FACE AU MONDE NUMÉRIQUE

Les différentes initiatives prises pour encourager le recours à l'administration en ligne posent la question de l'égalité des individus dans leurs rapports à l'État. Le risque serait en effet que le basculement de toutes les procédures administratives sur des supports électroniques réserve de plus en plus l'accès aux règles de droit et plus généralement aux documents administratifs à ceux qui bénéficient d'une connexion à Internet et ont les compétences pour s'orienter sur un réseau numérique.

Aucune règle de droit ne fait d'Internet le vecteur unique et exclusif d'un échange de données entre les citoyens et l'administration. La formulation retenue par l'ordonnance du 8 décembre 2005 encadre seulement la faculté qu'a l'administration de répondre par voie électronique à une demande formulée par cette même voie. Autrement dit, c'est le mode de communication utilisé par l'usager pour entrer en contact avec un service public qui autorise ce dernier à lui fournir une réponse recourant au même support.

(1) Cf. articles D. 15-6, D. 15-7 et D. 590 du code de procédure pénale.

Le déploiement du référentiel Marianne d'ici fin 2011 dans l'ensemble des 6 500 sites de l'État accueillant du public, selon l'objectif fixé par la RGPP, paraît garantir le maintien d'un accès « multicanal » à l'administration. Avoir une vision « globale » (1) de la relation avec l'usager est en effet au centre de cette politique lancée en 2005 et destinée à promouvoir la culture de l'accueil dans les services publics. Dans le cadre de ce programme, il est également prévu de renforcer la plateforme de renseignements téléphoniques « *3939* ».

La multiplicité des canaux ne signifie cependant pas une stricte identité des contenus ou des conséquences liées à l'utilisation de telle ou telle voie de communication. Plusieurs indices sembleraient justifier la crainte de voir le canal Internet se singulariser par rapport aux autres.

Il en va ainsi de la notion juridique de diffusion publique. Du fait de la portée de la diffusion assurée par le Web en comparaison avec celle d'un document papier, il a pu être considéré qu'une mise à disposition en ligne valait pour remplir une condition de publicité et, réciproquement, *« en l'absence de mise en ligne d'un document assortie de la possibilité de le télécharger gratuitement ou à un prix raisonnable, celui-ci ne [peut] être regardé comme faisant l'objet d'une diffusion publique* » (2)

Il a également pu être jugé que le refus par un tribunal de communiquer certains documents ne constituait pas une atteinte aux principes de transparence et de non-discrimination dans la mesure où ces textes étaient accessibles en ligne sur le site de *Légifrance* (3).

L'utilisation du média Internet pour la diffusion des circulaires est devenue une condition juridiquement nécessaire depuis le 1er mai 2009 ; aux termes de l'article 1er du décret du 8 décembre 2008 : « *Les circulaires et instructions adressées par les ministres aux services et établissements de l'État sont tenues à la disposition du public sur un site Internet relevant du Premier ministre. […] Une circulaire ou une instruction qui ne figure pas sur le site mentionné au précédent alinéa n'est pas applicable. Les services ne peuvent en aucun cas s'en prévaloir à l'égard des administrés.* » (4). Cette disposition est considérablement renforcée par l'article 2 du même décret qui dispose que les circulaires et instructions déjà signées sont réputées abrogées si, à cette date, elles ne sont pas reprises sur le site www.circulaires.gouv.fr. Le Conseil d'État a interprété strictement cette disposition en jugeant qu'une circulaire qui n'était pas en ligne au 1er mai 2009 devait être considérée comme abrogée même si celle-ci avait été postérieurement rendue accessible sur le site précité (5). La portée de ces dispositions semble ne pas avoir été saisie par l'ensemble des autorités

(1) Cf. référentiel Marianne, mai 2008, p. 5. http://www.modernisation.gouv.fr/fileadmin/Mes_fichiers/pdf/ReferentielMarianneV2log_10_mai_08.pdf
(2) Commission d'accès aux documents administratifs, rapport 2009, p. 37.
(3) CAA Versailles, 20 janvier 2009.
(4) Décret n° 2008-1281 du 8 décembre 2008 relatif aux conditions de publication des instructions et circulaires.
(5) CE, n°3347022, 23 février 2011.

concernées ; aussi, le Premier ministre a-t-il été conduit à diffuser, le 25 février 2011, une circulaire « *relative aux circulaires adressées aux services déconcentrés* » dans laquelle il rappelle ces règles [(1)].

Concernant la possibilité de différencier les procédures administratives selon le canal d'accès utilisé, le Conseil constitutionnel a été amené à se prononcer sur la constitutionnalité d'une disposition figurant dans le projet de loi de finances pour 2002 qui dispensait les contribuables, jusqu'à l'imposition des revenus de l'année 2003, transmettant leur déclaration de revenus par voie électronique de joindre à cette déclaration les reçus délivrés par les syndicats en vue d'obtenir une réduction d'impôt au titre des cotisations syndicales. Les requérants avaient estimé que cette disposition créait « une inégalité entre particuliers selon que ceux-ci transmettent leur déclaration de revenus par voie électronique ou par courrier » [(2)] et que, par conséquent, la disposition en question était contraire au principe d'égalité.

Le juge constitutionnel a estimé que la disposition contestée ayant pour simple objet de favoriser la déclaration des revenus par voie électronique, et ne dispensant pas de la production de ces pièces lors d'un contrôle fiscal ultérieur, n'était pas contraire au principe d'égalité [(3)]. Cette décision est éclairée par les commentaires suivants des *Cahiers du Conseil constitutionnel* : « *Les uns et les autres sont donc pareillement soumis à l'obligation de justifier les déductions demandées, seules variant les modalités de la vérification. Il en résulte que la différence de traitement entre télédéclarants (dispensés de produire les reçus concomitamment à leur déclaration) et les non télédéclarants (qui continuent à devoir joindre les reçus à leur déclaration) se justifie par une différence de situation en rapport avec l'objet d'intérêt général poursuivi par le législateur*. » [(4)]

Si l'on admet, plus que jamais, que la simplification des procédures administratives par le biais d'Internet est un objectif conforme à l'intérêt général et constitue un élément essentiel de la modernisation de l'État, il n'en reste pas moins que les différences de situation risquent de se transformer en inégalités, non pas tant au regard des obligations pesant sur les administrés, dont on peut penser qu'elles demeureront identiques quelles que soient les situations, mais en considération du principe de l'égalité des citoyens devant le service public. Il est ainsi souhaitable que l'ouverture d'un nouveau service en ligne ne se traduise pas par la fermeture d'un guichet mais, au contraire permette un redéploiement des personnels au profit de l'accueil et de l'accompagnement des administrés n'ayant pas recours à Internet. La CNIL a ainsi pu rappeler *« que le développement de l'administration électronique doit avoir pour objectif de mettre en place des outils de simplification des démarches administratives et d'amélioration des relations*

(1) Circulaire du 25 février 2011 relative aux circulaires adressées aux services déconcentrés, JO *du 1er mars 2011.*

(2) Cf saisine par soixante députés 2001-456 DC.

(3) Cf. Décision 2001-456 DC.

(4) Les Cahiers du Conseil constitutionnel, Cahier n° 12*, Commentaire de la décision n° 2001-456 DC du 27 décembre 2001.*

entre les usagers et l'administration, sans que ces outils soient exclusifs d'autres canaux d'échanges. » (1)

Cependant, de profonds motifs d'inquiétude demeurent. Ainsi, l'objectif fixé par la RGPP d'arriver à une administration « zéro papier » se concilie difficilement, si tant est qu'il doive être pris à la lettre, avec l'obligation de proposer des services identiques à tous les administrés, y compris à ceux pour lesquels le monde numérique n'est pas familier ou demeure inaccessible.

Dans deux délibérations en date du 25 mai 2010 (2), la CNIL a aussi pu exprimer son inquiétude sur le fait que la procédure à suivre pour fournir les pièces justificatives exigées par la SNCF afin d'obtenir la carte de réduction *Enfant Famille* ne soit accessible que sur Internet. Certes, la procédure en ligne simplifie beaucoup la démarche, mais pour écarter le risque d'une rupture d'égalité d'accès entre les familles, la CNIL recommande que soit mise en œuvre une procédure alternative à la demande de carte par voie électronique, en permettant par exemple de faire la demande de dossier au guichet, à partir d'une borne ou par voie postale. Il est en effet pour le moins paradoxal que l'obligation de passer par cette procédure exclusivement numérique soit imposée à des usagers pour lesquels l'accès au numérique est certainement le plus difficile ; les conditions de ressources auxquelles est liée l'obtention de la carte *Enfant Famille* réservent en effet cet avantage à une tranche de population dont une large partie n'a pas accès à Internet (3).

Le Conseil d'État avait, dès 1994, insisté sur le fait que « *la recherche de l'efficacité des services publics ne devrait jamais conduire à perdre de vue les objectifs de cohésion sociale auxquels il appartient à ces services de répondre, notamment par une interprétation à la fois rigoureuse et ouverte du principe d'égalité*. » (4) Le développement sur une grande échelle des services publics en ligne rend d'autant plus actuelle cette recommandation. À défaut, un profond déséquilibre risquerait de mettre à mal tout l'édifice administratif, comme si, selon les analyses de Mme Marie-Charlotte Roques-Bonnet, « *les différents supports permettant d'accéder à l'administration donnaient accès à des administrations distinctes, répondant à des objectifs et à des obligations différentes*. » (5)

---

(1) Cf Délibération n° 2008-578 du 18 décembre 2008 portant avis sur un projet d'arrêté relatif à la création d'un téléservice dénommé « mon.service-public.fr.

(2) Délibérations n° 2010-214 et n°2010-215 du 25 mai 2010 portant avis sur des projets d'actes réglementaires de la Caisse nationale d'allocations familiales et de la Caisse centrale de mutualité sociale agricole.

(3) Pour obtenir la carte Enfant Famille *en 2011, les ressources 2009 des demandeurs ne doivent pas dépasser 22 970 euros pour les familles avec un enfant et 28 271 euros pour les familles avec 2 enfants, plus 5 301 euros par enfant supplémentaire. Or, selon les estimations du Centre de recherche pour l'étude et l'observation des conditions de vie, moins de la moitié des personnes dont les revenus ne dépassent pas 18 000 euros par an sont équipés d'un ordinateur.*
Cf. La diffusion des technologies de l'information et de la communication dans la société française*, p. 71, CREDOC, décembre 2010, http://www.arcep.fr/uploads/tx_gspublication/rapport-credoc-2010-101210.pdf).*

(4) Conseil d'Etat, Les services publics, Rapport pour l'année 1994*, 1995, p. 128.*

(5) Cf. Le droit peut-il ignorer la révolution numérique ? *Michalon, 2010, chapitre I.*

Pour éviter de tels déséquilibres, la mission d'information en appelle au respect de l'approche dite « multicanal ». Dans cette perspective, chaque projet de dématérialisation devrait être lié à l'établissement d'un bilan sur l'accessibilité des documents et des procédures dans leurs versions non numériques.

Orientation n° 11 : maintenir un accès multicanal à l'administration

Garantir aux administrés que les procédures et les informations administratives dématérialisées demeurent accessibles par voie non numérique.

C. QUELLE GARANTIE D'ACCESSIBILITÉ À LONG TERME PRÉSENTENT LES DOCUMENTS ADMINISTRATIFS DÉMATÉRIALISÉS ?

Les usages d'Internet sont conçus pour l'immédiat ou le court terme. Les durées longues sont peu prises en considération de par la nature même du système. L'accroissement exponentiel des informations mises en ligne rend peu sensible au fait que, parallèlement, de nombreuses données disparaissent : des pages Web ne sont plus mises à jour, des sites ferment ou se transforment au gré de l'introduction de nouvelles techniques. Or lorsque les documents relèvent du champ de l'administration et sont dotés d'une valeur juridique, les droits qui y sont attachés doivent bénéficier de garanties à long terme ; à cette fin, l'accessibilité, la sécurité et la conservation au cours du temps de ces données ne doivent pas pouvoir être menacées. Dans le cas contraire il y aurait certainement à craindre un futur « âge sombre » du numérique, selon l'expression de certains spécialistes [(1)].

La question porte essentiellement sur la conservation des documents dits « natifs » n'existant que sous forme numérique. Le risque d'obsolescence du support est grand au vu de l'évolution très rapide des techniques. Comme l'expliquent les services du ministère de la Culture et de la communication « *archiver de manière pérenne une information numérique revient par conséquent à la rendre indépendante de son environnement d'origine afin de pouvoir la restituer lorsque cela sera utile dans l'environnement qui sera celui du temps de la restitution*. » [(2)]

La spécificité de cette démarche est qu'elle suppose que dans la conception même des documents soient prises en compte les conditions techniques de leur archivage.

Le projet de dématérialisation des actes authentiques s'est confronté à cette difficulté. Décrivant en 2008 la genèse de la création du minutier central électronique destiné à stocker les actes authentiques sur support électronique et à les conserver au moins soixante-quinze ans, le Conseil supérieur du notariat soulignait que *« la question de l'archivage d'actes notariés venus de tous les offices de France n'est pas anodine car il fallait garantir que des actes*

(1) L'expression de Digital dark age *est utilisée par les associations d'archivistes anglo-saxons.*
(2) Réponse à la question écrite n° 10501, Sénat, 17 décembre 2009.

authentiques électroniques signés aujourd'hui avec des logiciels informatiques de 2008 seront toujours accessibles et lisibles dans plusieurs dizaines d'années, quelles qu'aient été les mutations technologiques intervenues entre-temps. » (1)

En plus de mesures de sécurité renforcées dont fait l'objet le site de Venelles, à proximité d'Aix-en-Provence, où a été implanté le minutier central électronique, un reformatage régulier du répertoire est prévu ainsi que la conservation des minutes sous forme littérale (2) garantissant la pérennité de la lecture.

Or les mêmes difficultés vont se poser pour les actes de *e-administration* détenus par les services publics. Le plan de développement « France numérique 2012 » dispose que « *Le Gouvernement devra également assurer la conservation pérenne de la valeur de preuve des documents numériques ainsi produits, visant à maintenir leur lisibilité, intelligibilité, fiabilité et intégrité jusqu'au terme du délai durant lequel des droits y afférents peuvent exister.* » À cette fin, le plan prévoit dans son action n° 124, les dispositions suivantes :

« – Déterminer en coopération avec l'administration des archives compétente, dès la conception ou le choix d'un système d'information, le cycle de vie des données et documents qui seront traités par ce système ;

– élaborer des politiques d'archivage avant toute mise en œuvre d'un système d'archivage numérique sécurisé. »

Si la mission d'information a pu prendre la mesure de la complexité de ces différents problèmes qui touchent au droit des individus, il convient cependant de constater que la représentation nationale est mal informée des enjeux en débat et des défis à surmonter.

L'article 36 de la loi n° 2008-696 du 15 juillet 2008 relative aux archives disposait pourtant la remise au Parlement au plus tard un an à compter de la promulgation de la présente loi, puis tous les trois ans, d'un rapport portant sur les conditions de collecte, classement, conservation et communication des archives en France. Ce rapport devait présenter en particulier les mesures destinées à assurer la pérennité des archives numériques. Il est regrettable que cette disposition n'ait pas été appliquée puisqu'à ce jour aucun rapport d'application n'a été remis à la représentation nationale.

Orientation n° 12 : évaluer les procédures destinées à assurer la pérennité des documents administratifs dématérialisés

Dresser un bilan des actions entreprises et des questions tant techniques que juridiques que pose la conservation à long terme des documents administratifs dématérialisés.

(1) Signature du premier acte authentique sur support numérique*, dossier de presse, Conseil supérieur du notariat, 28 octobre 2008.*

(2) Le document est conservé au format ASCII qui est la norme de codage la plus ancienne et la plus largement compatible.

III. LE PARTAGE DES INFORMATIONS : DE NOUVELLES EXIGENCES

A. MIEUX GARANTIR LE DROIT D'ACCÈS AUX DONNÉES PUBLIQUES : LES *OPEN DATA*

1. Une demande nouvelle d'accès

Le développement du monde numérique a donné une portée nouvelle au droit d'information. Toute donnée peut dorénavant être échangée et exploitée avec la plus grande facilité grâce à Internet ; cette possibilité d'exploitation, qui est aussi source de création, est revendiquée avec force par de nombreux internautes qui demandent que l'accessibilité aux données soit systématiquement garantie – ce que les Anglo-Saxons appellent *open data*. L'exigence d'une « libération » de toutes les informations disponibles s'exprime aussi envers l'État, détenteur de l'ensemble des données relatives à l'action publique.

Cette revendication peut prendre une forme très médiatique, comme l'ont montré les différentes actions menées par le site WikiLeaks.

WIKILEAKS ET L'OPEN DATA

Créé en 2006, *WikiLeaks* s'est spécialisé dans la diffusion d'informations non publiques, obtenues de façon détournée. Il s'est rendu célèbre avec la publication d'une vidéo d'un raid aérien de l'armée américaine, le 12 juillet 2007, à Bagdad et la mise en ligne de plusieurs dizaines de milliers de documents secrets provenant de sources militaires et diplomatiques américaines relatifs aux guerres d'Afghanistan et d'Irak.

WikiLeaks se recommande du même principe de transparence que celui qui fonde la philosophie de l'*open data* : « Aidez-nous à maintenir les gouvernements ouverts », tel est le slogan de ses concepteurs. La fin justifiant les moyens, si l'État ne rend pas publiques ses données de sa propre initiative, il est légitime de le faire à sa place.

Au principe de libre accès des documents administratifs, la législation aménage des exceptions liées à deux préoccupations : le bon fonctionnement de l'État et la protection des données personnelles.

Si le principe de protection des données personnelles n'est pas contesté, celui d'une transparence absolue des activités de l'État fait l'objet de deux approches opposées. Pour les tenants d'une conception moderne de l'État, dans la tradition de Machiavel, l'État a besoin de se réserver des zones de secret dans les rapports de force qu'il entretient notamment avec les autres États. Pour les défenseurs d'une publicité intégrale de tous les ressorts des décisions politiques, aucune borne ne saurait être mise au droit d'information, *a fortiori* quand on dispose d'outils aussi performants qu'Internet pour les diffuser.

En tout état de cause, comme il en a déjà été fait mention dans le présent rapport, la fourniture de données ne prend un sens que si celles-ci sont analysées, vérifiées et interprétées. Sans ce travail professionnel, qui est celui des journalistes, toute donnée demeure muette.

De nombreuses données publiques ne mettent cependant pas en jeu le destin d'un État mais témoignent de son activité de gestion. Dans cette perspective, une politique d'ouverture des données publiques consistera à introduire des dispositifs de communication plus contraignants pour les

administrations et ouvrant de larges possibilités de réutilisation pour les internautes.

Dans le cadre de ses activités, tant celles tournées vers les usagers que celles relatives à son fonctionnement interne, l'administration produit en effet un grand nombre de données. Les catégories d'information peuvent être très diverses : des données de description du territoire (cartes, cadastre…) ; des fonds documentaires (études, réglementation, statistiques…) ; des données portant sur la décision publique (projets, enquêtes, délibérations, subventions, budgets…) ; des données relatives au fonctionnement des réseaux urbains (eau, énergie, transports, logistique, télécoms…) ; des données portant sur la localisation et les horaires d'ouverture des services et des commerces, sur l'occupation des ressources et des capacités (voirie, bâtiments, espaces, parkings…) ; des mesures (environnement, trafic…) ; des événements (culture, sports…) ; des informations touristiques, culturelles ; des données d'archives ; des données de surveillance ; des données électorales, etc. (1)

Le développement d'Internet suscite, pour plusieurs raisons, un intérêt croissant pour l'ensemble de ces *data*. En premier lieu, les facilités de communication offertes par le Web permettent d'une façon rapide et efficace le retour vers le public des informations conçues à son intention dans le cadre de l'activité des services publics. L'accès libre à ces données apparaît comme un juste retour des choses.

L*'open data* est aussi un outil de transparence de l'action publique dès l'instant où une obligation de mise à disposition pèse de façon générale sur l'administration. L'administration ne peut plus retenir par-devers elle les données qui dirigent son action ; elle doit les libérer ; ce faisant, elle expose les ressorts de ses décisions et permet de nourrir les débats citoyens. On pourra citer, par exemple, l'importance prise par toutes les données relatives à l'environnement et à la santé, qu'il s'agisse de l'impact des centrales nucléaires ou de celui des antennes relais.

Des considérations commerciales interviennent aussi. La réutilisation des données publiques est une source de valeurs pour les sociétés se spécialisant dans le traitement d'informations sous forme de bases de données. Les informations fournies par les administrations peuvent être traitées dans leur présentation, croisées avec d'autres, enrichies puis vendues à des clients ciblés.

Enfin, les nouveaux outils du Web 2.0, avec leurs très larges capacités d'innovation, fournissent à chaque internaute les moyens de faire une utilisation originale des données publiques. Une politique d'ouverture des données ne se limite pas à la mise en place d'un droit d'accès aux documents ; elle passe aussi par la reconnaissance d'un droit de réutilisation dans des conditions telles que l'inventivité des internautes, au principe même de l'Internet, ne soit pas entravée.

---

(1) Liste figurant sur la plateforme de données gérée par la ville de Rennes.

Dans un autre domaine, la plate-forme mobile d'Apple a ainsi suscité la création de plus de 100 000 applications. La culture « collaborative » paraît trouver là un champ privilégié d'expression.

L'ouverture des données publiques ne peut se faire que si ces différents intérêts n'entrent pas en contradiction.

2. L'adaptation de la législation

La directive européenne du 17 novembre 2003 relative à la réutilisation des informations du secteur public [(1)] a posé le principe général suivant : « *Les États membres veillent à ce que, lorsque la réutilisation de documents détenus par des organismes du secteur public est autorisée, ces documents puissent être réutilisés à des fins commerciales ou non commerciales […] Si possible, les documents sont mis à la disposition du public sous forme électronique.* »

Cette disposition trouve son fondement dans deux considérations. La première, d'ordre économique, met en avant la nécessité d'introduire des règles dans le marché de l'information. Les gisements de données publiques ont en effet une valeur marchande ; et comme l'explique le cinquième considérant de la directive « *L'amélioration des possibilités de réutilisation des informations émanant du secteur public devrait notamment permettre aux entreprises européennes d'exploiter le potentiel de ces informations et contribuer à la croissance économique et à la création d'emplois* ».

Le second justificatif est formulé dans le seizième considérant et se réfère aux droits fondamentaux : « *La publicité de tous les documents généralement disponibles qui sont détenus par le secteur public – non seulement par la filière politique, mais également par la filière judiciaire et la filière administrative – constitue un instrument essentiel pour développer le droit à la connaissance, principe fondamental de la démocratie. Cet objectif est applicable aux institutions, et ce, à tous les niveaux, tant local que national et international.* »

La directive a été transposée en droit interne français par l'ordonnance n° 2005-650 du 6 juin 2005 dont le contenu a été intégré au titre I^{er} de la loi 17 juillet 1978 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.

Ces nouvelles dispositions garantissent un droit d'accès à l'information, garant de la transparence de l'action administrative et de l'information des citoyens, et un droit de réutilisation « *à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus* » [(2)].

(1) Directive 2003/98/CE.
(2) Article 10 de la loi n° 78-753 du 17 juillet 1978.

Elles n'ont cependant pas modifié la nature des exceptions au droit d'accès telles que mentionnées à l'article 6 de la loi du 17 juillet 1978. Ne sont ainsi pas communicables les avis et les documents préalables d'un certain nombre d'instances administratives et juridiques ; les documents qui porteraient atteinte au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif, au secret de la défense nationale, à la conduite de la politique extérieure de la France, à la sûreté de l'État, à la sécurité publique ou à la sécurité des personnes, à la monnaie et au crédit public, au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente, à la recherche, par les services compétents, des infractions fiscales et douanières, et aux autres secrets protégés par la loi. Ces documents non communicables deviennent cependant consultables au terme des délais et dans les conditions fixées par le code du patrimoine [(1)].

L'article 13 de cette même loi précise que la réutilisation d'informations publiques comportant des données à caractère personnel est subordonnée au respect des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Par conséquent, l'utilisation qui peut être faite de ces données est liée soit au consentement de la personne intéressée, soit à une anonymisation du contenu. Dans ce dernier cas, comme le précise l'article 15, le coût de l'anonymisation peut être répercuté sur le montant des droits de redevance, l'administration n'étant pas tenue de communiquer le document si l'opération d'anonymisation entraîne des efforts « disproportionnés » [(2)].

L'article 17 oblige les administrations qui produisent ou détiennent des informations publiques à tenir à la disposition des usagers un répertoire des principaux documents dans lesquels ces informations figurent. Le répertoire doit préciser, pour chacun des documents recensés, son titre exact, son objet, la date de sa création, les conditions de sa réutilisation et, le cas échéant, la date et l'objet des mises à jour. Lorsque l'autorité administrative dispose d'un site Internet, elle rend le répertoire accessible en ligne.

Il est à noter que cette disposition est doublement limitée : elle ne vise que les données les plus importantes et ne se réfère qu'aux répertoires de données. Une circulaire du Premier ministre du 29 mai 2006 a ainsi pu reconnaître aux administrations une marge d'appréciation pour définir les documents qui doivent figurer dans les répertoires [(3)]. L'accessibilité en ligne de ces répertoires est en outre liée à l'existence d'un site Internet dont la création ne présente aucun caractère obligatoire.

---

(1) Cf articles L. 213-1 et L. 213-2 du code du patrimoine.

(2) Cf. article 40 du décret n° 2005-1755 du 30 décembre 2005 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, pris pour l'application de la loi n° 78-753 du 17 juillet 1978.

(3) Circulaire n°5156/SG.

Enfin, selon l'article 15, l'administration est autorisée à demander le versement de redevances dont l'assiette peut comporter les éléments suivants : les coûts de mise à disposition des informations, les coûts de collecte et de production des informations et « *une rémunération raisonnable de ses investissements comprenant, le cas échéant, une part au titre des droits de propriété intellectuelle*. »

Il convient de souligner que les documents communicables peuvent ne pas exister en tant que tels mais être issus de la consultation d'une base de données. L'accès aux documents couvre donc les demandes d'extractions de données par un traitement automatisé d'usage courant (1).

La mise à disposition des données géographiques a fait l'objet de dispositions législatives particulières. Par une directive en date du 14 mars 2007 (2), le Parlement européen a créé une infrastructure d'information géographique dans la Communauté européenne. Cette directive contraint les États membres à mettre gratuitement à la disposition du public, par l'intermédiaire d'un portail Internet, plus de trente catégories de données relatives aux territoires, *« aux fins des politiques environnementales communautaires et des politiques ou activités de la Communauté susceptibles d'avoir une incidence sur l'environnement.* » (3)

Pour être accessibles, ces données doivent être décrites à l'aide de « métadonnées » ; des fichiers contenant de grandes quantités d'information risqueraient en effet d'être inutilisables s'ils n'étaient pas accompagnés d'un index ou d'un catalogue.

Ce projet intéresse particulièrement les collectivités territoriales qui peuvent ainsi élaborer des cartes géographiques combinant différentes informations, ce qui constitue un outil précieux pour l'aménagement du territoire.

La directive Inspire a été transposée, malheureusement avec plus d'un an de retard, par ordonnance le 21 octobre 2010. (4)

---

(1) Cf. présentation de la CADA, sur son site Internet : http://www.cada.fr/fr/acces/frame.htm

(2) Directive 2007/2/CE du parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE).

(3) Article 1er de la directive INSPIRE : les catégories de données mentionnées dans les annexes de la directive sont les suivantes : référentiels de coordonnées ; systèmes de maillage géographique ; dénominations géographiques ; unités administratives ; adresse ; parcelles cadastrales ; réseaux de transport ; hydrographie ; sites protégés ; altitude ; occupation des terres ; ortho-imagerie ; géologie ; unités statistiques ; bâtiments ; sols ; usage des sols ; santé et sécurité des personnes ; services d'utilité publique et services publics ; installations de suivi environnemental ; lieux de production et sites industriels ; installations agricoles et aquacoles ; répartition de la population / démographie ; zones de gestion, de restriction ou de réglementation et unités de déclaration ; zones à risque naturel ; conditions atmosphériques ; caractéristiques géographiques météorologiques ; caractéristiques géographiques océanographiques ; régions maritimes ; régions biogéographiques ; habitats et biotopes ; répartition des espèces ; sources d'énergie ; ressources minérales.

(4) L'article 24 de la directive fixait le délai de transposition au plus tard au 15 mai 2009 (article 1er de l'ordonnance n° 2010-1232 du 21 octobre 2010 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière d'environnement).

Concernant la communication des données culturelles, des lignes directrices ont été suggérées par M. Bruno Ory-Lavollée dans un rapport remis en juillet 2009 au ministre de la Culture et de la communication. Des mesures favorisant « *la présence, la fréquentation et l'appropriation des données publiques culturelles sur les réseaux* » y sont préconisées [(1)].

3. Les réalisations

Au niveau national, les deux seules réalisations qui ont pu être mises en avant dans la réponse à une question écrite posée par notre collègue Lionel Tardy sur la situation des *open data* en France sont le portail d'information juridiques *Légifrance* et le portail de données statistiques de l'INSEE [(2)].

Dans ce même document il est précisé que « *Le plan France Numérique 2012 annoncé par le Gouvernement en octobre 2008 prévoit le développement d'un portail unique d'accès aux données publiques. Sa conception et sa réalisation ont été confiées à l'APIE [Agence du patrimoine immatériel de l'État]. Après une étude exploratoire menée en 2008 (enjeux juridiques, moyens et compétences nécessaires à sa réalisation), les travaux de conception ont été poursuivis en 2009 dans un cadre interministériel élargi à des personnalités qualifiées et à des utilisateurs en vue d'une mise en ligne fin 2010.* » Le Conseil de modernisation des politiques publiques, présidé par le Président de la République, présenté en Conseil des ministres le 30 juin 2010 par M. François Baroin, ministre du Budget, des comptes publics et de la réforme de l'État, a prévu l'ouverture de cette plateforme, dénommée « *Etatlab* », d'ici à juin 2011. Le Conseil des ministres du 24 novembre 2010 a repoussé ce délai à la fin de l'année 2011.

Mesurant très bien les difficultés à surmonter pour créer un site de données d'une dimension tout autre que ce que peut proposer une collectivité locale, la mission d'information s'est cependant interrogée sur la philosophie de la démarche suivie. Cette politique d'ouverture des données semble en effet avoir eu pour principal aiguillon, du moins dans un premier temps, la recherche exclusive d'une valorisation économique du patrimoine immatériel de l'État. Le compte rendu du Conseil des ministres du 24 novembre 2010 a ainsi précisé que le futur site de données publiques favoriserait « la réutilisation des données publiques par des acteurs privés », sans que les autres acteurs, à savoir la communauté des internautes, ne soient mentionnés ni qu'un principe général de transparence ne soit invoqué.

La mise en œuvre de la politique de mise à disposition des données publiques a été confiée, dans un premier temps, à l'APIE dont la première mission est, selon les termes de l'arrêté portant création de cette agence « *de proposer au ministre chargé de l'économie les orientations relatives à la stratégie de gestion*

(1) Partager notre patrimoine culturel. Propositions pour une charte de la diffusion et de la réutilisation des données publiques culturelles numériques*, 2009.*

(2) Question n° 56147, réponse publiée au Journal officiel *du 29 septembre 2009.*

des actifs immatériels de l'État, en vue d'assurer une meilleure valorisation de ce patrimoine » [1]. La valorisation dont il s'agit est ainsi explicitée par l'APIE : « *Cette politique doit poursuivre trois objectifs stratégiques : optimiser l'impact de la gestion du patrimoine immatériel sur l'économie ; tirer parti d'une meilleure valorisation des actifs pour moderniser les services publics, soutenir la conduite des politiques publiques au profit des usagers et contribuer au désendettement ; prémunir l'État et les usagers contre d'éventuels risques de détournement.* » [2]

L'action de coordination de l'APIE a conduit à la mise en ligne de quelques répertoires de fonds de données de services ministériels [3].

Cette démarche se distingue sensiblement de celle qui inspire, par exemple, le site du gouvernement américain *Data.gov*. Celui-ci se fixe pour but d'améliorer la capacité du public à trouver, à télécharger et à utiliser les bases de données. Cette politique se rattache à l'idée de promouvoir la démocratie participative en donnant à chaque citoyen les moyens de construire de nouvelles applications et de lancer ses propres recherches. L'ambition est grande : il s'agit, en atteignant un niveau inégalé de transparence, de renforcer « *la démocratie de la Nation et l'efficacité du Gouvernement*. » [4]

En Grande-Bretagne, le principe de la transparence de l'action publique est également le fil conducteur de l'organisation du site *data.gov.uk*. Partager les éléments d'information sur la base desquels se prennent les décisions politiques facilite la compréhension de l'action publique ainsi que sa critique. Une liste de principes que doit respecter toute politique d'ouverture des données a été rédigée le 26 juin 2010 [5]. À ce jour, 5 400 fichiers de données sont en ligne.

Le gouvernement australien a, lui aussi, créé un portail de données publiques [6].

C'est dans une perspective similaire que La Banque mondiale développe un programme de mise en ligne de bases de données statistiques, considérées comme « *un outil indispensable à une bonne gouvernance parce qu'elles permettent au public d'évaluer l'action des pouvoirs publics et de participer directement au processus de développement*. » [7]

Parmi les collectivités locales françaises, la ville de Rennes a été pionnière en créant une plateforme d'accès à des données portant sur les transports et la

---

(1) Arrêté du 23 avril 2007 portant création d'un service à compétence nationale dénommé « Agence du patrimoine immatériel de l'État », Journal officiel*, 12 mai 2007.*

(2) Cf. site de l'APIE : https://www.apiefrance.fr/sections/presentation_apie/missions/missions_de_l_apie

(3) Les services contributeurs ont été les suivants : Services du Premier ministre ; ministères de l'Économie et des finances ; de la Justice ; du Travail ; des Relations sociales ; de la Famille, de la Solidarité et de la ville ; de l'Alimentation, de l'agriculture et de la pêche ; de la Santé et des sports.

(4) Cf. site de DATA.Gov : http://www.data.gov/about.

(5) Onze principes sont formulés cf. http://data.gov.uk/blog/new-public-sector-transparency-board-and-public-data-transparency-principles.

(6) Cf. http://data.australia.gov.au/

(7) Cf. http://donnees.banquemondiale.org/a-propos/presentation

géographique. Trois objectifs sont avancés : « améliorer le quotidien des citoyens, accroître la transparence et créer de la valeur d'usage. » (1) La démarche collaborative est également mise en avant.

Se sont également engagées dans cette politique d'ouverture des données publiques, les villes de Brest, Nantes, Bordeaux, Montpellier et Marseille, ainsi que la ville de Plouarzel, dans le Finistère, qui a développé dès 2009 un outil de cartographie communale.

Enfin, la Ville de Paris a lancé un projet particulièrement ambitieux. Par deux délibérations du Conseil de Paris, en juin et décembre 2010, des séries de données possédées par la Ville de Paris ont été rendues accessibles sur le site *ParisData*, ouvert en janvier 2011.

Les premières mises en ligne ont porté sur des thèmes aussi divers que l'alignement des arbres, les concessions dans les jardins publics, les trottoirs, les murs, les clôtures, les équipements de proximité, le mobilier urbain, l'origine et les dénominations successives des voies parisiennes, les accès piéton, les accès véhicule, les seuils de porte, les rampes d'accès, les escaliers extérieurs, les terrasses, les listes des arrêtés municipaux d'insalubrité, les listes d'autorisation d'urbanisme, etc.

L'accès aux fichiers est lié à l'acceptation d'une licence qui garantit la liberté la plus large de réutilisation : liberté de partager, de copier, de distribuer et d'utiliser la base de données. *A contrario*, cette licence oblige les utilisateurs à procéder à un partage aux conditions identiques et empêche l'appropriation de la base.

L'internaute a la possibilité de laisser des commentaires sur la plateforme, faire des suggestions et expliquer quelle réutilisation des données il envisage.

Face à l'ensemble de ces initiatives, le retard pris par la mise en place du site *Etatlab* apparaît particulièrement regrettable. Surtout, les principes sur lesquels s'appuie la politique de l'ouverture des données possédées par l'État restent difficiles à appréhender, à l'exception de la seule dimension économique.

Si pour certains organismes, tels que l'IGN ou Météo France, la commercialisation des licences de réutilisation de données, représente une source de revenus, il ne semble pas que les évaluations financières sur les plus-values espérées d'une ouverture généralisée des données publiques soient suffisamment précises pour créer la dynamique qui fera que tous les secteurs de l'administration s'attacheront à rendre disponibles leurs fonds de données sur un portail unique.

(1) Cf. http://www.data.rennes-metropole.fr/notre-demarche/

4. Le futur portail d'accès aux données de l'État

Une décision récente laisse transparaître une réorientation profonde de la politique de libération des données publiques. Par décret en date du 21 février 2011 (1), « *Etatlab* » est devenue une mission, placée sous l'autorité du Premier ministre, chargée « *de la création d'un portail unique interministériel destiné à rassembler et à mettre à disposition librement l'ensemble des informations publiques de l'État, de ses établissements publics administratifs et, si elles le souhaitent, des collectivités territoriales et des personnes de droit public ou de droit privé chargées d'une mission de service public*. » Elle coordonne, en outre, « *l'action des administrations de l'État et apporte son appui à ses établissements publics administratifs pour faciliter la réutilisation la plus large possible de leurs informations publiques*. »

D'après la présentation qui en est faite sur le site du Gouvernement, le portail s'appellera *data.gouv.fr*, ce qui est une référence explicite aux modèles anglo-saxons. Il aura pour ambition de « *permettre à tous – journalistes, enseignants, chercheurs, développeurs, particuliers, etc. – d'accéder librement à l'ensemble des informations publiques dans des formats exploitables.*

« Toute la communauté des développeurs sera encouragée à développer des produits et des services innovants, comme des applications pour téléphone mobile à partir d'informations publiques géolocalisées mises à disposition sur data.gouv.fr.

« Dans un souci de transparence et de modernisation de l'État, "Etalab" mobilisera également certaines informations brutes afin de proposer de nouveaux services publics en ligne aux citoyens. » (2)

La mission d'information estime que cette redéfinition de la politique d'*open data* est un élément qui renforcera les droits des citoyens usagers d'Internet.

Sur le plan économique, si les profits pour l'État de cette politique ne doivent pas être négligés, les bénéfices à attendre proviendront moins de la vente de licences de réutilisation que de la mise en place d'un système ouvert de réemploi des données favorisant une multiplicité d'initiatives individuelles, créatrices d'emploi et de valeur.

La tâche reste cependant complexe. Par circulaire en date du 26 mai 2011 (3), le Premier ministre a précisé le cadre dans lequel se réalisera ce projet.

---

(1) Décret n° 2011-194 du 21 février 2011 portant création d'une mission "Etalab" chargée de la création d'un portail unique interministériel des données publiques.

(2) Cf http://www.gouvernement.fr/gouvernement/creation-d-etalab-le-portail-unique-de-reutilisation-des-donnees-publiques

(3) Circulaire du Premier ministre du 26 mai 2011 relative à la création du portail unique des informations publiques de l'Etat « data.gouv.fr » par la mission « Etalab » et l'application des dispositions régissant le droit de réutilisation des informations publiques.

Un recensement systématique des données disponibles est en premier lieu nécessaire. Plus de cinq ans après la transposition de la directive du 17 novembre 2003, trop peu de ministères se sont conformés à cette obligation, dont il convient par ailleurs de rappeler qu'elle vaut également pour les collectivités territoriales.

Pour coordonner cette action, la circulaire prévoit la nomination d'un interlocuteur unique du projet « Etatlab » dans chaque ministère.

Pour être effectif, l'accès aux données doit ensuite se faire dans un environnement technique qui puisse être partagé. Afin d'éviter la multiplication des formats de fichiers utilisés par les différents services administratifs, la circulaire recommande l'utilisation de formats favorisant l'interopérabilité des systèmes d'information.

Par ailleurs, la loi du 17 juillet 1978 ne prévoit pas la délivrance de licence en cas de réutilisation gratuite mais seulement si celle-ci donne lieu au versement de redevances [(1)]. Or, tant la Ville de Paris que l'APIE et quelques ministères concernés, notamment le ministère de la Justice, proposent des modèles de licence dans le cas d'une réutilisation gratuite. De telles licences permettent de préciser les conditions juridiques d'éventuelles réutilisations commerciales des données publiques. En particulier, la licence choisie par la Ville de Paris garantit une réutilisation libre et gratuite des données produites tout en écartant le risque d'un « pillage » [(2)] commercial des bases, le réemploi ou l'enrichissement des données ne pouvant faire l'objet d'une licence différente de celle qui a été initialement acceptée au moment de son extraction. Qu'il ne puisse y avoir réappropriation de la base des données devrait être un élément incitatif pour que les administrations partagent leurs fonds d'informations.

Sur cette question, la circulaire du 26 mai 2011 pose pour principe que *« la décision de subordonner la réutilisation de certaines de ces informations au versement d'une redevance devra être dûment justifiée par des circonstances particulières. Ces informations devront être au préalable inscrites sur une liste établie par décret.* » Il apparaît donc que la gratuité de la fourniture des informations constituera, dans l'avenir, le principe général. La circulaire prévoit qu'une licence gratuite sera proposée ; un groupe de travail a été créé pour en définir les termes.

La mise en ligne du portail « *data.gouv.fr* » est prévue pour la fin de l'année 2011. La mission d'information considère, au vu de l'importance d'un tel site d'information, que sa mise en place devra se faire dans la plus grande transparence. Le Parlement pourrait, en ce sens, être mieux informé de l'évolution du projet. Les moyens de fonctionnement du futur site devront être également suffisants pour assurer une communication des informations dans de bonnes conditions. Il est souhaitable, aussi, que les conditions particulières qui pourront justifier, selon la circulaire du 26 mai 2011, l'imposition de redevances soient

(1) Cf. article 16.
(2) Cf. intervention de M. Jean-Louis Missika, délibération du Conseil de Paris du 14 décembre 2010.

définies de façon la plus restrictive afin que le principe de gratuité conserve son effectivité la plus large.

Il est important, enfin que l'ouverture des données ne se réduise pas à une opération de communication ponctuelle, mais corresponde à une politique à long terme ; la mise en ligne doit constituer, sauf exception, le sort naturel des données administratives.

Pour autant, la politique d'ouverture des données ne saurait franchir les limites de la vie privée. La revendication de transparence qui nourrit la philosophie de *l'open data* n'est recevable que dans la mesure où elle porte sur l'action publique. C'est pourquoi, la mission d'information rappelle la nécessité de rendre anonymes les données personnelles détenues par les services publics avant toute publication. Si l'identification des personnes concernées par des données administratives devenait possible, même de manière indirecte, par exemple par croisement d'informations, il conviendrait de faire prévaloir le principe de protection de la vie privée sur celui de transparence. Les procédures en cours d'élaboration dans le cadre du projet « *Etatlab* » devront clairement prendre en compte cette exigence.

Orientation n° 13 : améliorer l'accès aux données publiques et en permettre la réutilisation tout en garantissant la protection des données personnelles

– Rendre plus effectif le droit d'accès aux données publiques en précisant les dispositions légales en vigueur (article 17 de la loi du 17 juillet 1978) afin que tous les organismes publics concernés recensent et rendent disponible en ligne l'ensemble de leurs données publiques communicables ;

– n'imposer une redevance pour la réutilisation des données que dans des cas exceptionnels ;

– obliger les administrations à recourir à des formats de fichiers qui permettent une exploitation documentaire des données qui y sont contenues ;

– garantir que l'ouverture des données publiques ne mettra pas en cause le principe de la protection des données personnelles.

B. ACCÈS AUX DONNÉES D'ARCHIVES ET PROTECTION DES DONNÉES PERSONNELLES

Le principe consistant à garantir le retour vers le public des données produites par les services publics ne saurait être absolu. La réutilisation d'archives publiques ne peut être autorisée ni au seul regard de la définition des données publiques telle que la pose la loi relative à l'accès aux documents administratifs ni en considération du seul respect des divers délais de communication des archives publiques tels que les fixe le titre I[er] du livre II du code du patrimoine [(1)]. Les

(1) Les archives publiques sont communicables de plein droit ; des délais dérogatoires allant de 25 à 100 ans sont fixés pour un certain nombre de documents.

autorisations d'exploitation d'archives dans lesquelles mention est faite de données personnelles restent subordonnées au respect des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, comme l'a rappelé la CNIL dans une délibération du 9 décembre 2010 (1).

Or le développement des services en ligne a provoqué un regain d'intérêt envers divers types d'archives pouvant contenir des informations d'ordre privé. Il s'agit, comme l'explique la CNIL, de services d'archives, d'associations ou de sociétés privées, notamment spécialisées dans la recherche généalogique, intéressés par « *la réutilisation et de la diffusion sur Internet des documents d'archives publiques, qui concernent non seulement les registres d'état civil et les questionnaires de recensement, mais aussi les registres d'écrou des prisons, des fichiers d'hospitalisation et des fichiers de recensement de certaines catégories de populations (prostituées, proxénètes, étrangers...).* » Citant des informations susceptibles d'être collectées telles que les acquisitions et pertes de la nationalité française, les condamnations pénales ou les données de santé, la CNIL souligne que, même si la personne concernée est décédée, les conséquences de leur publication sur la vie privée de personnes vivantes peuvent avoir « *des conséquences redoutables* ».

La CNIL a ainsi été conduite à rappeler que la constitution de bases de données et la réalisation d'index nominatifs de recherche à partir d'archives publiques contenant des fichiers diffusés sur Internet étaient liées à une autorisation ou à un avis de sa part, l'accord exprès des personnes pouvant difficilement être recueilli, soit en raison du nombre d'individus concernés soit du caractère ancien des documents traités.

La CNIL considère que certaines réutilisations de données personnelles contenues dans des documents d'archives sont à exclure.

Il en va ainsi des réutilisations des données dites sensibles (origines « raciales » ou ethniques, opinions philosophiques ou religieuses, appartenance syndicale, données relatives à la santé ou à la vie sexuelle), des données relatives aux infractions, condamnations et mesures de sûreté ainsi que des mentions apposées en marge des actes de l'état civil (reconnaissance d'un enfant naturel, adoption ou révocation d'adoption, francisation des noms ou prénoms après acquisition de la nationalité française, changement de sexe, mention « mort en déportation »).

Les deux premières catégories de données dont la réutilisation est prohibée renvoient aux interdictions posées par les articles 8 et 9 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La troisième catégorie est identifiée sur la seule base de l'appréciation faite par la CNIL des conséquences que la publication des données correspondantes pourrait avoir sur la vie privée et au regard des éventuels préjudices pour les ayants droit.

---

(1) Délibération n° 2010-460 du 9 décembre 2010 portant recommandation relative aux conditions de réutilisation des données à caractère personnel contenues dans des documents d'archives publiques.

Dans le cas des données ne relevant d'aucune des trois catégories précitées, la CNIL recommande qu'il soit procédé à une information générale, claire et complète portant sur la finalité de leur réutilisation, sur les catégories de données concernées et les destinataires du traitement. Le droit d'opposition, d'accès, de rectification et de suppression doit être effectif si les données concernent des personnes vivantes. Dans le cas contraire, dans le souci de préserver la mémoire des personnes, la CNIL recommande aux responsables de traitements qu'il soit fait droit aux demandes justifiées de suppression qui leur seraient présentées et d'assurer une information en ce sens.

Enfin la CNIL formule des recommandations concernant l'indexation des données. L'indexation constitue en effet le procédé qui valorise une base documentaire puisqu'elle permet de rassembler un grand nombre d'informations en fonction d'une seule requête. Si cette dernière porte sur le nom d'un individu, tous les éléments disséminés dans la base et indexés à ce nom peuvent être appelés et permettre de reconstituer une partie d'une biographie.

Des propositions d'indexation d'archives mises en ligne notamment par les départements ont déjà été faites par des sociétés commerciales. Sont visés en particulier l'état civil ancien, les recensements de la population et les registres de conscription militaire.

Mais l'Association des archivistes français a exprimé ses inquiétudes sur l'usage de telles techniques : « *si la concentration des données publiques nominatives et leur indexation sont autorisées, il sera possible à terme, en payant un abonnement et à partir d'un nom tapé dans un moteur de recherche, de connaître les personnes ayant porté ou portant encore ce nom et ayant connu, soit elles-mêmes, soit leurs ascendants directs, des ennuis judiciaires, des maladies mentales, des parcours sociaux ou politiques pouvant leur être opposés… Le profil familial d'un citoyen pourra ainsi être reconstitué et rendu accessible à tous dans toutes ses facettes (renseignements médicaux, données liées à la sexualité, instabilités matrimoniales, internements psychiatriques, incarcérations, positions militaires…)* » [(1)].

Aussi, la CNIL propose-t-elle de rendre impossible l'indexation par les moteurs de recherche des données relatives aux personnes nées depuis moins de 120 ans, la sécurité et la confidentialité du contenu des bases devant par ailleurs être garanties.

Cette dernière recommandation ne valant pas pour les personnes nées depuis plus de 120 ans, il convient semble-t-il d'en déduire que la CNIL considère dans ce cas comme acceptable la constitution de profils biographiques, sous la réserve d'ordre général qu'il n'y ait pas atteinte à l'intérêt d'ayants droit.

---

(1) La réutilisation des données nominatives ? Gare au fichage des individus ! *Communiqué de presse de l'Association des archivistes français, 6 juillet 2010. Cf. http://www.archivistes.org/La-reutilisation-des-donnees.*

Il convient cependant de souligner que les recherches à fins historiques, scientifiques ou statistiques sont écartées de l'ensemble de ce dispositif de contrôle, sous réserve que ces finalités puissent être caractérisées. Il en va ainsi, par exemple, des archives transférées aux services des Archives de France.

La délibération de la CNIL vaut non seulement comme une mise au point sur les limites de son champ de compétence par rapport à celui de la CADA mais, plus fondamentalement, elle rappelle que tant qu'un ayant droit peut se manifester, le mur de la vie privée ne s'effondre pas avec le temps et qu'il convient par conséquent de restreindre la publicité qu'assure la mise en ligne de données personnelles même si celles-ci sont anciennes.

La mission d'information constate néanmoins que le dispositif légal qui encadre l'ensemble de ces questions est complexe. Il en appelle en effet à une multiplicité des textes et repose sur l'action de deux autorités administratives indépendantes qui ont leur propre pouvoir d'interprétation ; il suscite naturellement les interrogations des administrations détentrices d'archives face au démarchage dont elles font l'objet de la part de sociétés commerciales ; ces dernières, pour leur compte, ne comprennent pas les entraves mises à leur liberté de commercer et estiment œuvrer dans un contexte marqué par une insécurité juridique préjudiciable ; enfin, les outils numériques étant très évolutifs, la capacité de numérisation des archives ne va aller qu'en augmentant et leur accès sur Internet deviendra de plus en plus facile.

L'ensemble de ces considérations conduit la mission d'information à suggérer que des initiatives soient prises par les ministères compétents afin d'évaluer les éléments en jeu au regard des droits de l'individu. Si le contexte juridique tel qu'issu de la délibération de la CNIL citée précédemment s'avérait perfectible, il conviendrait de porter le débat devant la représentation nationale et de proposer des dispositions législatives susceptibles de créer un cadre légal clair pour tous les acteurs.

Orientation n° 14 : évaluer les limites à poser à la réutilisation des données d'archives contenant des données personnelles

Clarifier le régime juridique de la réutilisation à des fins commerciales des archives contenant des données personnelles.

*
* *

En ouvrant de nouvelles perspectives de communication, en offrant de nouveaux moyens d'action politique et en instituant de nouveaux rapports entre l'individu et l'État, Internet se révèle être un instrument qui a profondément modifié les modes de coexistence à l'intérieur de la communauté humaine. Mais la mission d'information n'a pu que constater que dans chacun des secteurs où le recours aux outils numériques s'impose, des questions nouvelles émergent sur les

dérives que peuvent engendrer un échange et un traitement de l'information sans limites. Si tout moyen conduisant à briser les barrières entravant la liberté de communiquer, de penser, de savoir et de créer constitue un progrès des Lumières, il relève de cette même philosophie de maintenir d'autres barrières, protectrices de la personne : il en va ainsi de la protection de la vie privée, de la sécurité des échanges et de l'éducation que les mineurs doivent recevoir pour apprendre à utiliser ces nouvelles techniques.

TITRE DEUXIÈME

LE DROIT À UNE PROTECTION DANS L'UNIVERS NUMÉRIQUE

PREMIÈRE PARTIE : LE DROIT À LA VIE PRIVÉE : UNE PROTECTION À RÉINVENTER À L'ÈRE DU NUMÉRIQUE

La protection des données à caractère personnel et, plus largement, de la vie privée, fait partie intégrante des libertés et droits fondamentaux reconnus à chaque citoyen.

Lors de ses travaux, la mission d'information a été frappée à plusieurs reprises par le fait que, de plus en plus, les citoyens exposent leur vie privée sur Internet, notamment les plus jeunes, et qu'ils le font sans en avoir toujours conscience. Quand ils en prennent conscience et souhaitent mieux protéger leurs droits, ces internautes sont confrontés à des difficultés techniques et juridiques et se retrouvent alors relativement isolés face aux grands groupes de l'Internet, que sont *Google*, *Facebook* ou *Twitter*.

Avec le développement des réseaux numériques fixes et mobiles et, plus largement, des nouvelles technologies de l'information et de la communication, le débat sur la protection de la vie privée est sorti du milieu des experts pour devenir une question qui se pose à chacun.

La France a été précurseur en la matière il y a plus de trente ans. En effet, le respect de la vie privée passe d'abord par la manière dont sont collectées, exploitées et conservées les données personnelles par les entreprises, les administrations et les individus eux-mêmes. Elle a adopté, dès la fin des années 1970, une loi fondatrice – la loi « Informatique et libertés » – qui est la pierre angulaire de la protection des citoyens face aux traitements de données à caractère personnel.

De plus, ce cadre juridique a devancé et, parfois même inspiré, la mise en place de règles au niveau international et européen, comme la directive du 24 octobre 1995 sur la protection des données personnelles.

Mais il est aujourd'hui nécessaire d'adapter ces règles de protection de la vie privée aux évolutions technologiques ininterrompues de ces dernières années. Or, une approche commune en Europe est plus que jamais incontournable, notamment dans le cadre de la révision de la directive de 1995 engagée aujourd'hui par l'Union européenne.

I. LE PARADOXE DE LA VIE PRIVÉE À L'HEURE DE LA RÉVOLUTION NUMÉRIQUE : ENTRE PROTECTION ET EXPOSITION DE SOI

« *Pas de secret pour le boss* » [(1)], « *La fin de la vie privée* » [(2)], « *Internet menace-t-il notre vie privée ?* » [(3)]… Il n'est aujourd'hui pas rare de lire ici ou là de tels articles soulignant la peur diffuse que nourriraient les internautes à l'égard du respect de la vie privée sur le Web.

Or, ce sont les mêmes personnes qui, bien que craignant pour la protection de leur vie privée en ligne, n'hésitent pas, dans le même temps, à s'exposer et à divulguer leur intimité, notamment au travers des réseaux sociaux.

Il s'agit là de ce que les Américains appellent le « *paradoxe de la vie privée* », auquel la mission d'information a été confrontée tout au long de ses travaux. Un tel paradoxe appelle deux questions, auxquelles la mission s'est attachée à répondre : que reste-t-il de la notion de vie privée à l'heure des réseaux numériques ? Comment protéger une vie privée surexposée au regard des autres ?

A. QUE RESTE-T-IL DE LA VIE PRIVÉE…

Dans ses *Antimémoires*, André Malraux écrivait que « *la vérité d'un homme, c'est d'abord ce qu'il cache* », et si on adhère à cette conception de l'homme, on voit combien la vie privée et sa protection sont un enjeu fondamental. Mais cette notion est difficile à saisir et très largement dépendantes des représentations que les individus en ont.

Or, si la vie privée et le respect qui lui est dû nous semblent aujourd'hui des valeurs familières, il s'agit de notions modernes apparues au Siècle des Lumières qui a vu l'individu s'émanciper de la société et aujourd'hui remises en cause par le développement des nouvelles technologies.

1. Une découverte remontant au siècle des Lumières

Sous l'Ancien Régime, les Parisiens avaient l'habitude de se baigner nus dans la Seine. La reine de France accouchait en public, quand la maladie et la mort des grands personnages du Royaume étaient également publiques. Les annales de l'époque avaient fait un récit très détaillé du spectacle de la mort du roi Louis XIV emporté par la gangrène.

La littérature s'est également fait l'écho de cette confusion qui existait alors entre vie privée et vie publique, qu'Alexandre Dumas exprima en ces termes : « *outre le lever du roi et celui du cardinal, on comptait alors à Paris plus*

(1) Article de M. Christophe Alix paru l'édition de Libération *du 29 juin 2009.*
(2) Dossier paru dans La Revue*, n° 4, juillet-août 2010.*
(3) Dossier paru dans Science et vie micro*, n° 263, octobre 2007.*

de deux cents petits levers un peu recherchés. Parmi les deux cents petits levers, celui de Tréville était un des plus courus » (1).

Ni le secret de la santé ni celui des croyances n'étaient protégés en pareille situation. Les grands n'avaient pas droit, en principe, au respect de leur vie privée et l'intolérance religieuse de l'époque faisait que la liberté de conscience n'existait pas.

Au XVIII^e^ siècle, les philosophes des Lumières, puis au XIX^e^ siècle, les théoriciens du libéralisme politique vont fonder le régime démocratique sur l'existence de l'individu et l'exercice des libertés, légitimant ainsi la notion de sphère privée en opposition à la sphère publique, qu'au lendemain de la Révolution française, Benjamin Constant résumera en ces termes dans son discours prononcé en 1819 à l'Athénée : « *Il résulte de ce que je viens d'exposer, que nous ne pouvons plus jouir de la liberté des anciens, qui se composait de la participation active et constante au pouvoir collectif. Notre liberté à nous doit se composer de la jouissance paisible de l'indépendance privée* ».

« *Voilà donc la vie privée murée* », déclarait Royer-Collard, lors de la discussion parlementaire qui devait aboutir à l'adoption des grandes lois sur la presse de mai 1819. L'image d'un mur protégeant la vie privée est assez conforme à la société démocratique issue des Lumières qui « *reconnaît à l'individu le droit de disposer d'un espace privé, distinct de la vie collective de la communauté* » (2).

2. Une notion à géométrie variable qui recouvre trois invariants

Découverte et consacrée au Siècle des Lumières, la vie privée n'en reste pas moins une notion à géométrie variable suivant les époques, les pays et les représentations personnelles que s'en fait chaque individu.

L'imprécision des contours de la notion de vie privée a fait l'objet de nombreuses exégèses. En 1968, M. Robert Badinter soulignait déjà que « *s'agissant de la vie privée, […] plutôt que de définir le contenu, les juristes français se sont plus volontiers attachés à dépeindre le contenant. Depuis Royer-Collard, le célèbre mur de la vie privée se découpe bien nettement sur l'horizon juridique, mais quant au domaine qu'il enclôt, ses dimensions s'avèrent singulièrement variables* » (3).

Comme l'a relevé M. Fabrice Rochelandet, « *cette imprécision tient notamment aux statuts mêmes de cette notion qui peut désigner alternativement une revendication de la part des individus ou de la société civile, une situation de fait, une forme de contrôle, un droit garanti légalement ou encore une valeur morale en soi* » (4).

---

(1) Alexandre Dumas, Les Trois Mousquetaires*, Folio Classique, 2010, p. 26.*

(2) Rapport d'information n° 441, session ordinaire 2008-200, de M. Yves Détraigne et Mme Anne-Marie Escoffier sur le respect de la vie privée à l'heure des mémoires numériques, p. 11.

(3) Robert Badinter, Le droit au respect de la vie privée*, JCP G 1968, I, 2136.*

(4) Fabrice Rochelandet, Économie des données personnelles et de vie privée*, La Découverte, 2010, p. 7.*

Au-delà de cette imprécision, il est possible d'identifier les trois invariants qui, de manière constante, fondent la notion de vie privée conçue soit comme une capacité individuelle, soit comme la situation qui en résulte.

En premier lieu, la vie privée repose sur le secret, à savoir, pour Samuel Warren et Louis Brandeis, la vie privée est la « *capacité d'un individu à contrôler la collecte et l'utilisation de ses informations personnelles* » (1). À l'aune du secret, la vie privée mesure donc la capacité d'un individu à tenir secrets certains aspects de sa vie privée et à en contrôler leur divulgation. En effet, « *l'essence de la vie privée est ni plus (et certainement) ni moins que la liberté pour un individu de choisir pour lui-même le temps et les circonstances sous lesquels, et plus fondamentalement, la mesure dans laquelle ses attitudes, croyances, comportements et opinions doivent être partagés avec ou cachés des autres* » (2).

En deuxième lieu, la vie privée repose sur la tranquillité, que Samuel Warren et Louis Brandeis ont définie comme un « *droit à être laissé seul* ». En effet, comme l'a écrit le professeur Jean Rivero, « *la vie privée est cette sphère de chaque existence dans laquelle nul ne peut s'immiscer sans y être convié. La liberté de la vie privée est la reconnaissance, au profit de chacun, d'une zone d'activité qui lui est propre et qu'il est maître d'interdire à autrui* » (3). À l'aune de la tranquillité, la vie privée mesure la capacité d'un individu à ne pas être dérangé dans sa vie quotidienne et à se réserver une zone d'intimité qui échappe à toute immixtion extérieure. Elle diffère du secret dans la mesure où elle n'implique pas nécessairement la volonté de dissimuler des aspects de sa vie privée.

En troisième et dernier lieu, la vie privée peut se définir à la lumière de l'autonomie individuelle, à savoir « *le droit pour une personne d'être libre de mener sa propre existence comme elle l'entend avec un minimum d'ingérences de l'extérieur* » (4). En effet, comme l'a écrit l'économiste Hischleifer, la vie privée est « *le désir humain […] d'indépendance par rapport au contrôle des autres […], de contrôler sa propre personne et son propre temps* » (5). À l'aune de l'autonomie individuelle, la vie privée mesure l'aptitude d'un individu à prendre de son propre chef certaines décisions importantes concernant l'affirmation ou, au contraire, la dissimulation de certains aspects de sa vie privée à l'égard des tiers.

Ainsi définie dans ses trois dimensions, la vie privée doit bénéficier d'une protection juridique efficace pour être effective. Il s'agit du droit au respect de la vie privée qui doit permettre aux individus non seulement de garder secrets certains aspects de leur vie privée, mais également de se protéger contre toute

---

(1) Samuel Warren et Louis Brandeis, « The right to privacy », Harvard Law Review*, 1890, vol. 4, n° 5, p. 193-220.*

(2) Oscar M. Ruebhausen et Orville G. Brim., « Privacy and behavorial research », Columbia Law Review*, 1965, vol. 65, n° 7, p. 1184-1211.*

(3) Jean Rivero, Libertés publiques*, Dalloz, 1989, t. II, p. 76.*

(4) Conclusion Cabanes, CA Paris, 7e chambre, 15 mai 1970.

(5) Jack Hirshleifer, « The private and social value of information and the reward to inventive activity », American Economics Review*, vol. 61, n° 4, p. 561-574.*

intrusion extérieure et, enfin, de pouvoir prendre librement toutes les décisions afférentes à leur vie privée.

3. Un droit juridiquement consacré

La protection de la vie privée fait l'objet d'une préoccupation croissante. Ainsi, 65 % des Français redoutaient, en juin 2010, que leurs données personnelles soient réutilisées à des fins commerciales et 58 % se disaient intéressés par l'option « confidentialité » du navigateur Internet Explorer. Cette préoccupation concernant le respect de la vie privée est loin d'être récente. En effet, si les nouvelles technologies ont accru les risques en la matière (cf. *infra*), le droit au respect de la vie privée est garanti au plan national et européen depuis de nombreuses années.

En effet, comme l'expliquent MM. François Terré et Dominique Fenouillet, « *dans une société libre, chaque individu a deux vies : sa vie publique et sa vie privée. Vivant en société, l'individu ne peut prétendre faire échapper sa vie publique aux réflexions et aux regards d'autrui (...). [Mais] c'est en tant que telle que la vie privée doit être protégée contre les atteintes des tiers. La déformation de la vérité demeure alors répréhensible. Serait-elle conforme à la réalité, l'atteinte à l'intimité de la vie privée est condamnable* » [(1)].

En France, si la Constitution ne consacre pas, contrairement à certains de nos voisins européens [(2)], le droit au respect de la vie privée, la loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens a néanmoins inséré dans le code civil un article 9 qui dispose que « *chacun a droit au respect de sa vie privée* », les juges pouvant « *prescrire toutes mesures* [le cas échéant en référé] *telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée* ».

La garantie juridictionnelle de ce droit ne s'est toutefois pas accompagnée d'une définition législative de la vie privée. C'est donc la jurisprudence qui, au fil des arrêts, a dessiné les contours et précisé le contenu de cette notion.

Le Conseil constitutionnel a ainsi considéré que la liberté individuelle proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen [(3)] impliquait le respect de la vie privée [(4)], avant de reconnaître que « *la liberté d'aller et venir et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789* [étaient] *des libertés constitutionnellement garanties* » [(5)]. Au

---

(1) François Terré et Dominique Fenouillet, Droit civil*, Dalloz, coll. Précis, 6e éd., 1996, p. 88 et 89.*

(2) C'est notamment le cas de l'Espagne, dont la Constitution du 29 décembre 1978 dispose dans son article 18 que « le droit à l'honneur, à l'intimité personnelle et familiale et à sa propre image est garanti. […] La loi limitera l'usage de l'informatique pour garantir l'honneur et l'intimité personnelle et familiale des citoyens et le plein exercice de leurs droits *».*

(3) « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression *».*

(4) Décision 99-416 DC du 23 juillet 1999 sur la loi portant création d'une couverture maladie universelle.

(5) Décision n° 2003-467 DC du 13 mars 2003 sur la loi sur la sécurité intérieure.

niveau européen, la Cour de justice des communautés européennes a également reconnu, dans un arrêt *E. Stauder contre Ville d'Ulm* du 12 novembre 1969, qu'en raison de la tradition constitutionnelle commune aux États membres, le droit au respect de la vie privée comme un principe général du droit communautaire.

Le juge judiciaire, en faisant application de l'article 9 du code civil, s'est, pour sa part, efforcé de définir le contenu de cette notion de vie privée. Ainsi, à titre d'exemple, il a jugé que la vie sentimentale d'une personne présente un caractère strictement privé et l'article 9 du code civil interdit de porter à la connaissance du public les liaisons véritables, ou imaginaires, qui lui sont prêtées [(1)]. En matière de santé, la vie privée est étroitement protégée par le juge qui a rappelé que des informations couvertes par le secret médical ne pouvaient être communiquées à un tiers sans que soit constaté l'accord de la victime ou son absence d'opposition à la levée du secret [(2)]. S'agissant enfin des échanges, le juge européen a considéré que la réception de communications indésirables ou choquantes constituait une ingérence dans la vie privée, tout en reconnaissant cependant aux utilisateurs des systèmes d'échanges de courriers électroniques la faculté de réduire ces inconvénients par des filtres [(3)].

B. … À L'HEURE DE LA RÉVOLUTION NUMÉRIQUE ?

Ainsi garantie et protégée en droit, la vie privée doit à l'heure des réseaux et mémoires numériques faire face, dans les faits, à de nouvelles menaces qui, sous l'attrait du progrès technologique, ne manquent pas de séduire les utilisateurs.

Au nombre de ces nouveaux risques pour la vie privée, figurent en première place les réseaux sociaux, qui sont aujourd'hui un phénomène massif, que nul ne peut ignorer, y compris sur son lieu de travail. D'autres technologies moins visibles et plus insidieuses, comme les puces *RFID*, la géolocalisation ou le ciblage publicitaire, s'installent également dans la vie quotidienne de tout un chacun, parfois à leur insu.

1. Le Web 2.0, un village planétaire où tout se sait

Comme l'a souligné le sociologue Dominique Cardon, « *Internet fait apparaître dans le demi-jour les conversations qui se déploient sous l'espace public traditionnel. Nos relations quotidiennes sont émaillées de bavardages, d'avis et d'humeurs à propos de tout et de rien. […] Un des aspects les plus originaux de la transformation qu'apporte Internet à l'espace public traditionnel est de rendre visible et de garder en mémoire ce babil souvent insignifiant* » [(4)]. Ce nouvel espace d'expression, c'est le Web 2.0.

---

(1) TGI de Paris, 2 juin 1976.
(2) Cass., Civ., 2e, 19 février 2009.
(3) CEDH, 13 novembre 2007.
(4) Dominique Cardon, La démocratie Internet, Promesses et limites*, La République des idées, Seuil, 2010, p. 53.*

Cette expression de Web 2.0 a été employée pour la première fois en 2005 par M. Tim O'Reilly en vue de désigner une mutation du Web statique vers le Web participatif, qui se caractérise par un ensemble de sites, d'applications et d'usages de l'Internet créant une interface entre les internautes et ce, quel que soit leur degré de connaissance technique, en vue d'échanger des contenus entre eux, particulièrement par le biais des réseaux sociaux tels que *Facebook*, *Viadeo* ou *Twitter* (cf. *infra*). Pour reprendre les termes de M. Dominique Cardon, le Web 2.0 est « *une immense cour de récréation, le coin de la rue, le comptoir où l'on cause* » (1).

Le Web 2.0 ne se résume pas aux seuls réseaux sociaux. Si Internet est devenu un village planétaire où tout se sait, c'est également sous l'action de géants de l'Internet, comme *Google* ou *Yahoo* qui proposent, outre l'accès à leur moteur de recherche, des services très diversifiés permettant aux internautes de publier et mettre en ligne des contenus et, de la sorte, dévoiler sur la « Toile » une partie de leur vie privée.

À titre d'illustration, la société *Yahoo ! France* propose, comme l'a indiqué, Mme Brigitte Cantaloube, directrice générale, lors de son audition (2), un service de moteur de recherche, mais également des outils de communication (*Yahoo Mail* et *Yahoo ! Messenger)*, un service *Questions/Réponses* qui permet aux internautes d'interroger les autres membres de la communauté et, enfin, un service de partage de photographies (*Flickr*). Selon M. Dominique Cardon, 69 % des photographies publiées sur *Flickr* sont rendues publiques par celui qui les met en ligne, alors même que celui-ci a la possibilité de les réserver à un espace privé (3).

La société *Google* n'est pas en reste. Outre son service de messagerie électronique *Gmail* et son moteur de recherche qui enregistre 2,5 milliards de requêtes chaque jour et 30 000 requêtes par seconde et qui représentait en 2009 67,5 % du marché mondial, *Google* propose, avec son service *Google Street View*, lancé en France en juin 2008, une vue panoramique à 360° des rues de nos agglomérations que des véhicules équipés d'appareils de prise de vue – les *Google cars* – ont photographiées. Nombre de personnes ont alors vu mises en ligne, sans leur consentement, les photographies de leur habitation. Il est vrai que les images ont été conservées pendant un an à partir de leur publication, afin de laisser le temps aux personnes concernées de s'opposer à la mise en ligne de la photographie de leur domicile. Mais, comme l'a relevé M. Alex Türk, « *le particulier se voit contraint de déclencher une procédure pour éviter que le monde entier puisse repérer le lieu où il habite* » (4).

Ainsi, le Web participatif, pour offrir à ses utilisateurs de nouveaux services toujours plus innovants, s'immisce de manière croissante dans la vie

---

(1) Ibid.
(2) Audition du 14 septembre 2010.
(3) Rapport d'information n° 441 de M. Yves Détraigne et Mme Anne-Marie Escoffier, op. cit.*, p. 33.*
(4) Alex Türk, La vie privée en péril*, Des citoyens sous contrôle, Odile Jacob, Paris, p. 15-17.*

privée des individus. Certains y voient « *une révolution de type anthropologique : la protection de la vie privée n'y est plus considérée comme un élément essentiel au bien-être des peuples et la part secrète dont tout individu est constitué ne semble plus mériter d'échapper au grand déballage* ».

2. L'exposition consciente et volontaire de soi : le spectre des réseaux sociaux

Cette immixtion croissante dans la vie privée s'appuie principalement sur les nouvelles formes de sociabilité dont le Web 2.0 permet l'expression par le biais des *blogs* ou des réseaux sociaux, tels que *Facebook*, *MySpace*, *Twitter*, ou *Google Buzz* (1). Le risque que ces derniers font peser sur la vie privée est cependant d'une nature singulière, puisqu'il s'appuie sur la complicité active des internautes qui s'y exposent consciemment et volontairement. Le fondateur de l'hégémonique *Facebook*, M. Marc Zuckerberg, ne l'exprimera pas autrement en 2004, dans un « chat » publié par *Business Insider* : « *J'ai près de 4 000 adresses, mails, photos… Les gens me les ont données. J'ignore pourquoi ils me font confiance, putain d'abrutis !* » (2).

Comme l'ont indiqué M. Yves Détraigne et Mme Anne-Marie Escoffier dans leur rapport sénatorial sur le respect de la vie privée à l'heure des mémoires numériques, « *les réseaux sociaux sont des services proposés par des sociétés de l'Internet et qui offrent aux individus la possibilité, d'une part, de se constituer une page personnelle (un « profil ») sur laquelle ces derniers déposent un certain nombre d'informations les concernant et, d'autre part, d'entrer en communication avec d'autres utilisateurs (appelés « contacts » ou « amis ») du même réseau avec lesquels ils peuvent échanger des messages ou des fichiers (photos, vidéos, etc.)* » (3).

Ils ont connu ces dernières années un développement extraordinaire, analysé en ces termes par le sociologue Dominique Cardon : « *en quelques années à peine, les plateformes de réseaux sociaux ont conquis une place centrale non seulement dans les usages de l'Internet, mais aussi dans nos vies, nos relations d'amitié, nos amours. Le tournant est saisissant. En 2005, parmi les dix sites à plus forte audience dans le monde, on comptait des services de vente en ligne et des grands portails commerciaux comme* eBay, Amazon, Microsoft *ou* AOL. *Depuis 2008, ceux-ci ont disparu du classement au profit de* YouTube, MySpace, Facebook *et* Wikipédia. *En 2010, on dénombrait 500 millions d'utilisateurs de* Facebook *dans le monde, dont 17 millions en France* » (4).

S'agissant plus particulièrement de la France, le centre de recherche pour l'étude et l'observation des conditions de vie (CREDOC) estime qu'en 2010, 36 % de la population française étaient membres d'un réseau social, alors qu'ils

(1) La société Google a lancé en février 2010 son propre réseau social dénommé Google Buzz.
(2) In *Alex Türk,* La vie privée en péril*, Des citoyens sous contrôle, Odile Jacob, Paris, p. 116.*
(3) Rapport d'information n° 441 de M. Yves Détraigne et Mme Anne-Marie Escoffier, op. cit.*, p. 31.*
(4) Dominique Cardon, op. cit.*, p. 54.*

n'étaient que 23 % dans ce cas en 2009. La proportion atteint presque huit personnes sur dix parmi les 12-25 ans et le phénomène est loin de rester cantonné aux plus jeunes : en 2010, les taux de participation aux réseaux sociaux ont ainsi progressé de 21 points chez les personnes entre 25 et 40 ans et de 22 points chez les ouvriers. De tous les usages d'Internet et des technologies numériques que le CRÉDOC suit depuis quinze ans dans ses enquêtes, la participation aux réseaux sociaux est la pratique qui s'est diffusée le plus rapidement : en une année seulement (entre 2009 et 2010), 7 millions de personnes en France ont rejoint un réseau social virtuel [(1)].

Mais l'ampleur du phénomène des réseaux sociaux se mesure moins à l'aune du nombre de personnes inscrites que de la masse de données personnelles qui y sont mises en ligne. Ainsi, selon le rapport précité de M. Yves Détraigne et Mme Anne-Marie Escoffier, on estime qu'un utilisateur de *Facebook* est en moyenne relié à 120 « amis » et qu'un profil-type sur *Facebook* contient en moyenne 40 informations à caractère personnel, parmi lesquelles figurent nom, date de naissance, sexe, opinions politiques et religieuses, préférences sexuelles, livres et films préférés, parcours scolaire, universitaire et professionnel, le tout accompagné de photographies et parfois même de vidéos.

Comme l'analyse le CRÉDOC dans son étude sur la diffusion des technologies de l'information et de la communication, « *cet engouement est révélateur de profonds changements dans la manière de communiquer et d'échanger avec ses proches : ces pratiques permettent de tisser de nouveaux liens entre les individus, ils renforcent certaines relations tout en redéfinissant les contours des différents cercles amicaux* » [(2)].

Mais, ce phénomène social pose le problème de l'exposition et de la protection de la vie privée de chacun. En effet, s'il est incontestable que toutes ces données personnelles sont mises en ligne par les utilisateurs eux-mêmes, on doit reconnaître que, dans le même temps, le fonctionnement même des réseaux sociaux les encourage à dévoiler un grand nombre d'informations sur leur vie privée. Or, une fois qu'ils ont mis en ligne ces informations, les utilisateurs sont confrontés à un risque de perte de contrôle sur l'utilisation de leurs propres données : d'une part, ces informations peuvent être vues ou lues par des personnes ne figurant pas parmi les contacts de cet utilisateur ; d'autre part, elles peuvent être réutilisées à leur insu par d'autres membres de ce réseau. Aujourd'hui, il suffit d'être membre du réseau social *Facebook* et de naviguer sur d'autres sites liés pour laisser, là où on passe, des traces bien plus détaillées que la simple adresse de l'ordinateur. Ainsi, toute information confiée par l'utilisateur à *Facebook* peut échapper à son propriétaire.

Ce risque avait d'ailleurs été soulevé par les commissaires à la protection des données, réunis lors d'une conférence internationale à Strasbourg en

(1) CREDOC, La diffusion des technologies de l'information et de la communication dans la société française*, décembre 2010, p. 106.*

(2) Ibid.

octobre 2008, qui rappelaient qu'« *il peut être très difficile, et parfois même impossible, de retirer complètement l'information du Web une fois qu'elle est publiée : même après la suppression sur le site d'origine (par exemple le site de réseau social), des copies peuvent être conservées chez des tiers ou des prestataires de service de réseaux sociaux. Les données personnelles des profils peuvent également « déborder » du réseau quand elles sont indexées par des moteurs de recherche* ».

L'exposition au regard de tous de tant d'informations personnelles induit, selon le sociologue Dominique Cardon, le passage d'une « *surveillance institutionnelle de l'État et des entreprises* », autour de laquelle s'était organisé, lors de l'examen de la loi *Informatique et libertés* à la fin des années 1970, le débat sur la protection des données à caractère personnel, à une « *surveillance interpersonnelle d'un nouveau type* ». En effet, « *avec la démocratisation des instruments d'observation que les plateformes relationnelles distribuent à leurs utilisateurs, l'exposition de soi est un risque que l'on prend d'abord devant ses proches, ses voisins, ses collègues ou son employeur* ». Fort de ce constat, M. Dominique Cardon conclut, d'une part, que « *Facebook est sans conteste l'emblème de ce nouveau panoptisme horizontal* » et, d'autre part, que « *la prophétie deleuzienne du passage d'une société disciplinaire à une société de contrôle prend […] tout son sens, puisque de manière décentralisée, chacun ne cesse de surveiller les autres et soi-même* » (1).

Il n'est ainsi aujourd'hui pas rare de voir un spécialiste du recouvrement se servir des réseaux sociaux pour retrouver des débiteurs changeant trop souvent d'adresse postale. Les détectives privés ne sont pas en reste : « *Facebook est très efficace, bien plus utile que les fichiers de police. La CNIL ne nous met pas de bâtons dans les roues. Les gens racontent toute leur vie en détail. Et le plus fou : les informations sont exactes, la plupart ne mentent même pas* », confie l'un deux sous couvert d'anonymat (2).

Conscients de ces risques d'atteintes à la vie privée, les concepteurs des réseaux sociaux ont mis en place des paramètres de confidentialité – ou « *privacy settings* » – permettant aux utilisateurs de contrôler eux-mêmes les données qu'ils mettent en ligne et, dans cette perspective, de définir les différents niveaux de visibilité et d'accessibilité de leur profil. En dépit de ces avancées, ces paramètres de confidentialité présentent certaines limites.

En premier lieu, comme l'ont rappelé dans leur rapport M. Yves Détraigne et Mme Anne-Marie Escoffier, « *les conditions générales d'utilisation des réseaux sociaux font périodiquement l'objet de modifications, lesquelles ne sont qu'imparfaitement notifiées à leurs utilisateurs* » (3). La société *Facebook* a d'ailleurs été, à intervalles réguliers, critiquée pour son attitude jugée « *cavalière* »

(1) Dominique Cardon, La démocratie Internet, Promesses et limites*, La République des idées, Seuil, 2010, p. 64-65.*

(2) Cyril Frey, « Les nouvelles servitudes volontaires », in La Revue*, n° 4, juillet-août 2010, p. 98.*

(3) Rapport d'information n° 441 de M. Yves Détraigne et Mme Anne-Marie Escoffier, op. cit.*, p. 33.*

envers les données privées de ses utilisateurs et a été notamment accusée de ne pas être suffisamment claire sur la manière dont fonctionnent ses options de confidentialité. Une lettre de protestation a même été adressée en mai 2010 par les 27 États de l'Union européenne, qui jugeaient « *inacceptable que* Facebook *ait modifié le réglage par défaut sur sa plate-forme de socialisation au détriment des utilisateurs* ». En outre, avec ses homologues européens, la CNIL a demandé à *Facebook* de mettre en place des profils protégeant davantage par défaut la vie privée des utilisateurs.

Tel n'est pas toujours le cas. Ainsi, lorsqu'un utilisateur de *Facebook* invite par courriel un de ses contacts à rejoindre le réseau social, *Facebook* adjoint, outre l'invitation, un certain nombre d'informations portant sur des personnes déjà inscrites sur *Facebook* et susceptibles d'êtres connues de l'individu démarché. De la même manière, après le lancement en février 2010 du réseau social *Google Buzz*, les utilisateurs de comptes de messagerie électronique *Gmail* se voyaient attribuer automatiquement – sans consentement, ni information préalable – une liste de contact d'amis qui comprenait des personnes avec lesquelles ils avaient communiqué par courriels. À cette occasion, neuf autorités de protection des données ont adressé une lettre commune de protestation à *Google* : « *Votre lancement récent de l'application de réseau social buzz […] a été fait dans le mépris des normes et des lois fondamentales en matière de protection de la vie privée. En outre, ce n'est pas la première fois que votre entreprise omettait de tenir compte du respect de la vie privée en lançant de nouveaux services* ».

La mission d'information a auditionné le représentant de *Facebook*, M. Richard Allan, directeur Europe de la politique publique [(1)]. On doit constater que la présentation idyllique que le représentant de cette puissante société a faite de la politique de protection des données personnelles menée par *Facebook* a laissé songeur plus d'un membre de la mission et elle a paru être l'expression au mieux d'une grande innocence au pire d'un cynisme somme toute choquant. La mission n'a pas été beaucoup plus convaincue par les propos – moins lénifiants cependant – tenus par les représentants de *Google* le même jour.

Les exemples de *Facebook* et de *Google* soulignent l'urgence qu'il y a en France et, plus largement, en Europe, à encadrer l'utilisation qui est faite par les réseaux sociaux des adresses courriels détenus par les utilisateurs. L'Allemagne a été pionnière en ce domaine. En effet, en janvier 2011, elle a contraint *Facebook* à informer les tierces personnes de la collecte et l'utilisation par le site de leur adresse électronique. Les personnes concernées peuvent alors refuser, leur courriel étant alors crypté sur les serveurs de *Facebook* de manière à ne plus être utilisée à cette fin, ni à être repérée. La mission propose de suivre l'exemple allemand, en obligeant tous les réseaux sociaux à limiter les « recherches d'amis » à partir du carnet d'adresses mèl. de leurs utilisateurs, en offrant aux personnes concernées la possibilité de s'opposer à une utilisation de leur adresse courriel.

(1) Audition du 8 septembre 2010.

Orientation n° 15 : protéger l'intimité des internautes en limitant les « recherches d'amis » sur les réseaux sociaux

Sur le modèle de l'exemple allemand, contraindre les réseaux sociaux à limiter les « recherches d'amis » à partir du carnet d'adresses mèl. de leurs utilisateurs, en offrant aux personnes concernées la possibilité de s'opposer à une utilisation de leur adresse mèl.

En deuxième lieu, le recours par les utilisateurs à ces paramètres de confidentialité reste encore trop faible. Ainsi, des études réalisées aux États-Unis en 2007 ont montré que moins d'un tiers des utilisateurs de *Facebook* prenaient connaissance des conditions générales d'utilisation du site avant de s'y inscrire. Finalement, 61 % des utilisateurs de ce réseau social choisissent, en dépit des outils de paramétrage qui leur sont offerts, de se rendre visibles à tous. Ce désintérêt pour la politique de confidentialité peut notamment s'expliquer par son manque de clarté et de visibilité à l'intérieur du réseau social.

En troisième lieu, ces paramètres de confidentialité ne semblent pas suffisants pour garantir la sécurité des données mises en ligne par les utilisateurs. Ainsi, en avril 2010, ce sont 1,5 million de comptes *Facebook* qui ont été piratés avec toutes les données qui y étaient associées, et proposés à la revente pour 25 à 45 dollars les 1 000 contacts selon leur intérêt. L'avertissement figurant au point 15 de la déclaration des droits et responsabilités de *Facebook* est, à cet égard, très clair : « *Nous ne garantissons pas que* Facebook *soit sûr et sécurisé* ». Dans ces conditions, le risque d'une usurpation d'identité n'est pas mince.

En quatrième et dernier lieu, les paramètres de confidentialité protègent les seuls utilisateurs du réseau social et laissent ainsi démunies les personnes qui, ayant choisi de ne pas être membres d'un tel réseau, voient leur vie privée exposée au regard de tous. En effet, rien n'empêche un individu de publier des informations nous concernant sur son profil, sans notre autorisation, voire même sans même que nous en soyons informés.

En somme, la vie privée et sa protection sont encore loin de connaître sur les réseaux sociaux toutes les garanties que les utilisateurs sont en droit d'attendre. Soucieuse de porter sur ces plateformes d'échanges une appréciation objective, la mission a adressé, le 14 décembre 2010, par la voix de ses rapporteurs et de son président, un questionnaire à la société *Facebook*. En dépit d'une lettre de rappel envoyée le 30 mars 2011, l'entreprise n'a pas souhaité répondre sur des sujets qui sont pourtant censés être au cœur de ses préoccupations quotidiennes et de sa démarche commerciale – vie privée, droit à l'oubli, sécurité, protection des mineurs – et sur lesquels on peut légitimement penser qu'elle a nécessairement une réponse. La mission regrette bien évidemment un tel silence, dont elle ne peut pas complètement exclure qu'il s'agit déjà d'un aveu…

S'il faut résumer en quelques mots les relations complexes et conflictuelles qui tantôt unissent, tantôt opposent les réseaux sociaux et les règles de respect de la vie privée, il est important de se référer aux propos de par M. Alex Türk, président de la CNIL, pour qui les réseaux sociaux « *éprouve[nt] toujours*

quelque peine à accroître l'efficacité de ses dispositifs permettant d'assurer la protection des données personnelles et de la vie privée parce que, tout simplement, la culture de la société est entièrement vouée à l'exploitation de celles-ci au profit du développement d'activités commerciales » (1).

Une prise de conscience s'est toutefois opérée tant de la part des pouvoirs publics que des utilisateurs eux-mêmes. S'agissant du réseau *Facebook*, les premières actions en faveur de la protection de la vie privée remontent à la fin de l'année 2008. Ainsi, *Facebook* a suscité, le 28 février 2010, la première journée mondiale sans *Facebook*, réaction à la cyberdépendance et à l'intrusion publicitaire, stigmatisées par les initiateurs de l'événement. Par ailleurs, le 31 mai 2010 a été décrété *Quit Facebook Day* – « le jour où quitter *Facebook* »

– qui a vu 30 000 départs du réseau social. En septembre 2010, une manifestation pour la protection de la vie privée sur *Facebook* a réuni plusieurs milliers de personnes.

La conférence mondiale des commissaires à la protection des données et de la vie privée, réunie à Strasbourg en octobre 2008, a de son côté adopté une résolution consacrée à la protection de la vie privée dans les services de réseaux sociaux. Dans cette résolution, les commissaires préconisaient la mise en place d'une large campagne d'information impliquant le plus grand nombre possible d'acteurs publics et privés, et destinée à prévenir les risques liés à l'utilisation des réseaux sociaux. Dans leurs recommandations, ils insistaient notamment sur la nécessité pour ces services de respecter pleinement la législation du pays dans lequel se trouve l'utilisateur, sur l'octroi d'un droit effectif d'accès et de rectification sur l'ensemble des données personnelles détenues par le réseau social ou encore sur l'éducation des utilisateurs au respect de la vie privée des autres.

3. Les nouvelles technologies dans le monde du travail : une nouvelle approche des relations professionnelles

Le monde du travail n'échappe à cette vague déferlante des réseaux sociaux, où ces derniers ont généré des tensions croissantes entre employeurs et salariés. Or, ces tensions s'inscrivent toutefois dans un mouvement plus large de remise en cause de la frontière entre vie professionnelle et vie privée sous l'effet des nouvelles technologies, comme le constatent MM. Jean-Emmanuel Ray et Jean-Paul Bouchet, dans leur article « *Vie professionnelle, vie personnelle et TIC* » : « *Quarante ans après le premier échange de courriel entre l'université de Los Angeles et celle de Stanford, les toujours renouvelées technologies de l'information et surtout de la communication effacent peu à peu la frontière spatiale mais aussi temporelle de notre bon vieux droit du travail façon Boulogne-Billancourt ou Sochaux : elles sont même l'un des principaux facteurs de la confusion grandissante vie professionnelle/vie personnelle d'aujourd'hui* » (2).

---

(1) Alex Türk, op. cit.*, p. 134.*

(2) Jean-Emmanuel Ray et Jean-Paul Bouchet, « Vie professionnelle, vie personnelle et TIC », Revue droit social*, 1er janvier 2010.*

Aujourd'hui, utiliser Internet pour son travail ou pour suivre une formation est une réalité pour environ un quart des Français [1]. Or, les nouvelles technologies menacent la vie privée du salarié, avant même qu'il soit embauché, une fois qu'il est sur son lieu de travail et, sa journée de travail terminée, alors qu'il est à son domicile familial.

En effet, il n'est plus rare qu'une décision de recrutement se fonde certes sur le *curriculum vitae* du postulant, mais également sur toutes les traces numériques que ce dernier a disséminées sur Internet. En effet, comme l'analysent MM. Jean-Emmanuel Ray et Jean-Paul Bouchet, « *nombre de recruteurs n'ont plus à rechercher longtemps des renseignements un peu spéciaux : ils trouvent sur* Facebook *ou* MySpace *des informations professionnelles mais aussi très privées gracieusement fournies par les candidats eux-mêmes. Scandaleux au temps du CV anonyme ? Mais partent-ils le matin en laissant grande ouverte la porte de leur appartement ? Il faut donc se* Googleliser *et se* Facebooker *réciproquement avant un entretien d'embauche. On y apprend très en amont beaucoup de choses que la Halde ne saura jamais, et que le candidat ne sait pas lui-même car ce sont des tiers – ses « amis » – qui évoquent les multiples facettes de sa vie personnelle. […] La plupart laissent en ligne des informations, photos et vidéos vraiment personnelles qui les suivront… longtemps : tous ces bons mots, photos et autres vidéos croustillantes resteront gravés dans le marbre du numérique* » [2].

En juin 2010, on estimait à 47 % la part des directeurs des ressources humaines reconnaissant recruter *via Facebook*. Aux États-Unis, ce pourcentage s'élevait, à la même époque, à 45 % et 38 % d'entre eux reconnaissaient avoir rejeté un *curriculum vitae* en raison des données mises à dispositions sur les réseaux sociaux. Le président de la CNIL, M. Alex Türk, a d'ores et déjà soulevé cette question, rappelant que « *c'est vers la fin de l'année 2008 que sont parvenues* [à la CNIL] *les premières plaintes concernant le recours, par les directeurs des ressources humaines et les cabinets de recrutement, au réseau* Facebook*, dans le cadre de leurs procédures de sélection des candidats* » [3]. Cette pratique semble d'ailleurs généralement admise, puisque « *dans un premier temps, ils* [les directeurs des ressources humaines] *ont nié vigoureusement cette évolution pour admettre peu après, devant l'évidence, que le phénomène s'était généralisé au motif que 50 % des CV qui leur étaient remis étaient tronqués. En réalité, la « googuelisation » ou la « facebookisation » leur offre une approche « dynamique », « en situation », et plus « spontanée » des candidats que la lecture d'un CV* » [4].

Une fois le salarié recruté, la menace que font peser sur sa vie privée les nouvelles technologies de l'information est loin de disparaître. En effet, les salariés n'hésitent plus, sur leur lieu de travail, à utiliser leur ordinateur

---

(1) CREDOC, La diffusion des technologies de l'information et de la communication dans la société française*, décembre 2010, p. 115.*

(2) Jean-Emmanuel Ray et Jean-Paul Bouchet, op. cit.

(3) Alex Türk, op.cit*. p. 126-127.*

(4) Ibid.

professionnel pour se connecter à un réseau social ou utiliser leur messagerie électronique personnelle. Comme l'analysent MM. Jean-Emmanuel Ray et Jean-Paul Bouchet, « *le collaborateur a pointé, il est assis à sa table de travail, mais il ne travaille pas. Hier au téléphone avec ses enfants ou refaisant le monde avec ses collègues devant la machine à café, il préfère aujourd'hui discuter sur MSN,* Twitter *ou retrouver ses copains d'avant sur* Facebook *ou d'autres réseaux dits « sociaux » : activités nettement plus chronophages que sncf.com ou courdecassation.fr, sans parler d'éventuels téléchargements de moins en moins légaux depuis les lois dites Hadopi 1 de juin 2009 et surtout Hadopi 2 du 28 octobre 2009* » [(1)]. En juin 2010, on estimait que 70 % des cadres détenaient un compte *Facebook* et que 58 % des utilisateurs de *Facebook* se connectaient depuis leur lieu de travail.

Comment, dans ces conditions, est-il possible, tant pour l'employeur que le salarié, de concilier vie professionnelle et vie privée et de tracer une ligne de partage claire et précise entre ces deux univers ? La jurisprudence de la Cour de cassation est, à cet égard, très éclairante. En effet, dans un arrêt de principe, *Nikon*, du 2 octobre 2001, la chambre sociale a posé le principe du respect de la vie privée au bureau, en considérant que « *même au temps et au lieu de travail, le salarié a droit au respect de l'intimité de sa vie privée ; celle-ci implique en particulier le secret des correspondances ; l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ».

La chambre sociale de la Cour de cassation a également, dans cet arrêt *Nikon*, établi une *summa divisio* entre vie privée et vie professionnelle sur le lieu de travail, en se fondant sur le titre « personnel » qui est donné aux courriels et aux fichiers. Faisant application de cette jurisprudence, elle, a estimé, dans un arrêt du 17 mai 2005, que *« sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé* ». Prolongeant cette jurisprudence, elle a également considéré, dans un arrêt du 18 octobre 2006, que « *les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence* ».

Si la jurisprudence a dessiné une ligne de partage relativement claire entre vie privée et vie professionnelle, il ne fait aucun doute, pour la plupart des utilisateurs des réseaux sociaux, comme *Facebook*, que ces derniers sont des univers privés. La justice commence pourtant à penser le contraire. Le 19 novembre 2010, le conseil des prud'hommes de Boulogne-Billancourt a en

(1) Jean-Emmanuel Ray et Jean-Paul Bouchet, op. cit.

effet estimé que le licenciement de deux salariés qui avaient dénigré leur employeur sur *Facebook* était fondé. Si cette décision faisait jurisprudence, les membres du réseau social seraient désormais prévenus : tout propos diffusé sur *Facebook* pourrait être retenu contre eux. Le droit français punit l'employé qui dénigre son employeur, quel que soit le support auquel il recourt.

Il se trouve que les réseaux sociaux constituent des lieux d'échanges « hybrides », entre espace public et privé. Si les prud'hommes n'ont pas, en France, encore réellement tranché sur le statut privé ou public de *Facebook*, le jugement rendu le 19 novembre 2010 tient au fait que l'espace dans lequel les personnes accusées s'étaient exprimées était ouvert aux amis d'amis pouvant ainsi être assimilé à un espace public. Un autre paramétrage de leur « profil » aurait peut-être conduit à une autre décision. Cette décision ne remet nullement en cause la jurisprudence précitée de la Cour de cassation : les échanges par message électronique appartiennent, eux, à la sphère privée dès lors qu'ils sont titrés « *personnel* » et l'atteinte au secret des correspondances privées, comme le courriel, est un délit puni d'un an d'emprisonnement et de 450 000 euros d'amende.

Une fois sa journée de travail achevée, le salarié rentre à son domicile, qui semble *a priori* relever de la seule sphère privée. Or, les nouvelles technologies de l'information ont, une nouvelle fois, modifié la ligne de partage entre vie privée et vie professionnelle, la seconde prenant le pas sur la première en dehors du temps de travail. Comme l'analysent MM. Jean-Emmanuel Ray et Jean-Paul Bouchet, « *dans le temple de l'intimité de leur vie privée (leur* home*), pendant leurs « temps de repos », pendant leurs « vacances » où ils sont censés exclusivement « vaquer à des occupations personnelles », de plus en plus nombreux sont les salariés tentant simplement d'éviter la submersion en éclusant leurs courriels professionnels. Or, en y répondant à 23 heures ou dimanche midi, ils génèrent à leur tour des réponses : au XXI*e *siècle, en nos temps si modernes, un courriel est forcément urgent ; et comme il est urgent, il devient important et ne peut attendre plus de deux heures. La courtoisie minimum du millénaire précédent (ex. : ne pas appeler après 20 heures) semblant avoir disparu avec le téléphone fixe où l'on risquait de tomber sur le conjoint ronchon, c'est dans un total mépris de la vie privée et familiale que des cadres sont dérangés à leur domicile parfois jusqu'à 23 heures par des managers mais aussi des collègues voire des collaborateurs esseulés et/ou stressés. Non sans quelque ambivalence : disposer de tels bijoux technologiques fait l'admiration des enfants, rend jaloux le conjoint, et se faire appeler à 22 heures 33 pour régler les problèmes de la planète peut être valorisant pour certain(e)s. Cercle donc extrêmement vicieux que cette « Toile » au sens arachnéen* » [(1)].

Le CRÉDOC estime ainsi qu'en 2010, près d'un Français sur quatre effectuait du travail à domicile, sur son ordinateur ou sur internet, même si ce phénomène concerne davantage les cadres (53 %) que les employés (14 %). En

(1) Ibid.

effet, plus le niveau de diplôme est élevé, plus l'interconnexion entre la sphère professionnelle et le domicile est importante.

4. Des individus tracés avec ou sans leur consentement : le panoptique de la géolocalisation

Si le phénomène des réseaux sociaux suscite tout à la fois l'enthousiasme et la crainte, la mission s'est, tout au long de ses travaux et à l'instar du président de la CNIL, posé la question de savoir si « *depuis peu, […] le développement des applications de géolocalisation ne constitue pas l'évolution la plus préoccupante* » (1).

En effet, les dispositifs de géolocalisation connaissent un développement sans précédent, faisant peser sur la protection de la vie privée des risques nouveaux. La multiplication de ces différentes technologies – tels le GPS (« *global positioning system* » ou, en français « *système de positionnement mondial* »), le Wifi, les puces *RFID* (« *radio frequency identification* » ou, en français, « *radio-identification* »), etc. – conduit à s'interroger sur d'éventuelles atteintes à la liberté pour les citoyens de circuler librement et anonymement, d'autant plus que se développent les recherches en matière de nanotechnologies et qu'il sera sans doute possible, dans quelques années, d'intégrer ces dispositifs de géolocalisation à des éléments invisibles pour l'œil humain.

UN PARAPLUIE TECHNOLOGIQUE À ROISSY

« 2 juillet 2020 au matin, départ pour New York. »

« Pour me rendre à Roissy, j'ai pris le RER grâce à mon pass Navigo (traçage possible). Dans le hall d'accueil du terminal 2E, j'ai acheté un polar avec ma carte bancaire (traçage possible), puis j'ai retiré quelques dizaines d'euros au « Point argent » (traçage possible) avant d'adresser un texto à l'un de mes amis. À présent, une affiche publicitaire me hèle sur mon système *Bluetooth*, mais je ne donne pas suite. Certes, plusieurs caméras, aussi bien dans les couloirs du métro qu'aux abords et à l'intérieur de l'aéroport, ont enregistré mes déplacements mais je n'y ai pas prêté attention. J'échappe d'ailleurs au dispositif biométrique « Parafes », car il ne concerne que les passagers qui empruntent les navettes sur le territoire français.

« Avant de procéder à mon enregistrement, je vérifie que tout est bien en ordre. J'ai rempli le formulaire ESTA (*electronic system for travel authorization*) délivré par le ministère de la Sécurité intérieure américain (j'ai bien fourni les renseignements demandés concernant mon vol, ma destination, mon adresse mail ainsi que mon état de santé, ça devrait aller). Lors de ma réservation, j'ai également fourni les renseignements demandés par Air France (dispositif PNR – *passenger name record*) qui les transmettra aux autorités américaines (qui produiront un profil me concernant, sur la base d'un *scoring* – indicateur de risque). Ces données concernent le pays et l'aéroport d'où je viens, les modalités de paiement, mon agence de voyages, mais aussi mes habitudes alimentaires…*A priori*, je n'ai aucune raison de figurer sur une *no fly list* (« liste de passagers interdits de vol »), contenant environ 65 000 noms de personnes jugées indésirables sur le territoire américain. Quant à mon passeport biométrique (photographie et empreintes digitales numérisées), je suis à jour.

« Au contrôle, je préfère passer au scanner corporel plutôt que de me soumettre à la palpation. Pour le moment les autorités françaises ont résisté aux pressions de leurs homologues qui

(1) Alex Türk, op.cit.*, p. 51.*

aimeraient les voir renoncer au système reposant sur les ondes millimétriques au profit des rayons X (mais j'y aurai droit à mon arrivée à New York).

« Je feuillette un magazine en salle d'embarquement sous le regard de caméras spéciales équipées d'un système de détection des « comportements erratiques ». Puis, finalement, disposant d'un peu de temps, je décide de passer d'une boutique à l'autre. À la caisse, la personne devant moi vient d'être rejointe par un vigile qui lui demande instamment de regagner au plus vite sa porte d'embarquement. C'est une application, désormais généralisée, du système « OPTAG » couplant une géolocalisation du passager « flâneur » permettant de le repérer (grâce à une puce *RFID*, insérée dans le billet de transport) avec une vidéo panoramique qui permet de le suivre dans ses déplacements jusqu'à l'intervention du vigile…

« Que l'on me comprenne bien, il ne s'agit pas de contester la politique mise en œuvre par les responsables de la sécurité de l'aéroport de Roissy ni d'aucun autre aéroport français, confrontés à d'évidents problèmes de sécurité collective. Cette petite excursion virtuelle vise simplement à faire prendre conscience du fait que si chacun de ces dispositifs se justifie en soi, en revanche leur concentration sur un site et leur combinaison créent un phénomène nouveau susceptible de poser de réelles questions quant à notre capacité à exercer encore, dans les années à venir, notre liberté d'aller et venir. Ce scénario me paraît d'autant plus intéressant que, d'une part, les dispositifs évoqués ne sont pas encore tous opérationnels et que, d'autre part, il préfigure sans doute ce qui se passera aussi dans les gares, les stades, les salles de spectacle, etc. Et pourquoi pas, un jour, dans les lycées, les universités, les hôpitaux ?

« L'enjeu commence à apparaître : comment donner au citoyen les clés lui permettant de comprendre l'essence de ces phénomènes, de mesurer le risque qu'ils induisent pour l'exercice de ses libertés, et d'exprimer ses attentes en matière de régulation et de réglementation de la part des pouvoirs publics ? Il faut, au préalable, pour avancer dans cette voie, évaluer ces phénomènes technologiques. C'est ce que je me propose de faire ici. »

Alex Türk, *La vie privée en péril, Des citoyens sous contrôle*, Odile Jacob, Paris, p. 15-17.

En effet, comme le souligne à juste titre M. Alex Türk, « *les dispositifs installés font de plus en plus appel à des techniques de miniaturisation et donc deviennent de moins en moins visibles* ». La géolocalisation se marque ainsi par l'introduction croissante des nanotechnologies qui vont décupler la puissance des systèmes de surveillance. Dans moins de dix ans, il sera possible de créer des systèmes d'informations qui entendront, verront à distance et qui seront si petits - échelle du milliardième de mètre – qu'on ne pourra plus jamais être certain de savoir où ils se trouvent. Ces technologies changeront immanquablement nos comportements : si chacun est conduit à faire attention en permanence à ce qu'il dit et fait, tout le monde finira par se ressembler. Les nanotechnologies ne vont pas aboutir à un changement de degré mais à un changement de nature des problèmes de protection de la vie privée. Aujourd'hui, face au système *Big brother*, les individus ont encore la possibilité de se révolter. Mais face au développement des nanotechnologies, face à ces milliards de *Little brothers*, il ne fait aucun doute que cela sera beaucoup plus difficile.

Or, la mission partage le constat de M. Alex Türk, selon lequel « *le problème est que l'opinion publique est loin d'être consciente de ce phénomène et ce, d'autant qu'elle ne l'observe pas avec le recul nécessaire puisqu'elle y participe, par exemple, par l'usage du téléphone de dernière génération* » [(1)]. De manière générale, la géolocalisation est un bon exemple d'une situation où les

(1) Ibid.

individus succombent à une technologie parce qu'elle est disponible. Ainsi, beaucoup de maternités songent à mettre en place un système de surveillance avec bracelets électroniques ou puces *RFID* pour prévenir les rapts d'enfants. La presse a également évoqué le projet d'une crèche parisienne, associative et privée, envisageant d'expérimenter la géolocalisation avec des puces *RFID* intégrées dans un vêtement spécial remis aux enfants. D'autres usages sont susceptibles de se développer dans les prochaines années : surveillance des adolescents et des personnes âgées, contrôle du trafic sur les autoroutes grâce à la reconnaissance des plaques d'immatriculation…

Les acteurs de l'Internet ont, d'ores et déjà, développé de multiples applications de géolocalisation. Ainsi, le logiciel de cartographie *Google Maps* offre une fonctionnalité dite *Latitude* qui permet en temps réel à une personne d'indiquer à ses contacts où elle se trouve et de localiser ces derniers grâce à leur téléphone portable. Actuellement développé dans une trentaine de pays pour environ 100 millions d'abonnés, ce service peut être désactivé ou suspendu à tout moment par l'utilisateur, qui a également la possibilité de ne pas être localisé par certains de ses amis.

Cependant, en « traçant » les individus dans leurs moindres déplacements, les techniques de géolocalisation ne sont pas sans risque pour la protection de la vie privée. À l'heure où elles tendent à se banaliser dans le grand public, la mission estime qu'il est plus que jamais nécessaire de mieux les encadrer. Il apparaît ainsi souhaitable que le Parlement s'engage dans la voie d'une modification de l'article 25 de la loi du 6 janvier 1978 précitée [(1)], de manière à définir un régime d'autorisation, par la CNIL, de la mise en œuvre de traitements de géolocalisation. En effet, en l'état actuel du droit, ces derniers ne font l'objet que d'une seule déclaration. Comme le souligne M. Alex Türk, « *dès lors, la situation est la suivante : la CNIL, saisie d'une déclaration correctement agencée, visant à mettre en œuvre un dispositif de géolocalisation, est dans l'obligation de délivrer le récépissé et ne peut donc s'opposer* a priori *à la réalisation du projet même si elle juge que de sérieux problèmes se posent sur le fond* » [(2)].

Soumettre les systèmes de géolocalisation à un régime d'autorisation permettrait de développer l'action de surveillance que met, d'ores et déjà, en œuvre la CNIL sur la conformité des pratiques de géolocalisation aux dispositions actuelles de la loi du 6 janvier 1978, comme l'a montré le récent contrôle mené sur l'activité de collecte de données techniques sur les réseaux Wi-Fi, mise en œuvre par la société *Google* aux fins d'offrir des services de géolocalisation [(3)].

---

(1) Cet article définit le régime d'autorisation par la CNIL des traitements automatisés portant sur des données personnelles.

(2) Alex Türk, op.cit.*, p. 52-53.*

(3) Le 17 mars 2011, la CNIL a prononcé à l'encontre de la société Google une amende de 100 000 euros, à la suite de contrôles ayant révélé divers manquements comme la collecte de données Wi-Fi à l'insu des personnes concernées et la captation de données dites « de contenu » (identifiants, mots de passe, données de connexion, échanges de courriels) – la CNIL avait constaté que les véhicules déployés sur le territoire français par Google enregistraient non seulement des photographies, mais aussi des données transitant par les réseaux sans fil Wi-Fi de particuliers.

Orientation n° 16 : pour des systèmes de géolocalisation autorisés et non plus simplement déclarés auprès de la CNIL

Modifier l'article 25 de la loi du 6 janvier 1978, de manière à soumettre la mise en œuvre des traitements de géolocalisation à un régime d'autorisation par la CNIL et non de simple déclaration comme cela est actuellement le cas.

5. Les puces *RFID* : entre invasion et droit au silence

Parmi les technologies sur lesquelles s'appuie le développement de la géolocalisation, figurent les puces *RFID* – en anglais « *Radio Frequency Identification* » ou, en français, identification par radiofréquence. Cette technologie permet d'identifier et de localiser sans contact des objets ou des personnes grâce à une micropuce (également dénommée étiquette ou tag) qui dialogue par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à une dizaine de mètres.

Le développement des puces *RFID* donne naissance à des usages toujours plus nombreux et dans des domaines les plus variés : nouveaux titres d'identité sécurisés (comme les passeports), nouveaux titres de transports en commun (comme le pass Navigo de la RATP), traçabilité des produits dans la distribution, connaissance instantanée du contenu et du prix d'un caddie de supermarché, lutte contre la contrefaçon. La technologie *RFID* peut ainsi apporter un certain confort en permettant, par exemple, d'améliorer la ponctualité des vols dans l'hypothèse où les cartes d'embarquement, dotées de cette technologie, permettent de localiser rapidement les passagers en retard.

Lors de son audition, M. Bernard Benhamou, délégué aux usages de l'Internet, a rappelé l'utilité sociale de ces puces *RFID*. De nombreux services pourront être développés au service des consommateurs concernant la vie d'un produit. Ainsi, en faisant communiquer une denrée alimentaire avec un espace de stockage réfrigéré ou une cuisine, les puces permettront de vérifier les dates de péremption des produits. De manière générale, elles rendront possible une complète traçabilité en matière de sécurité alimentaire, permettant ainsi de retirer précisément les produits défectueux. Il sera plus nécessaire d'attendre de détecter le numéro de série pour mettre en place des mesures de rappel. Les puces auront également une utilité sociale en matière d'économies d'énergie. En effet, une puce installée sur tous les appareils électriques permettra une meilleure maîtrise de la consommation énergétique, en déclenchant, par exemple, un appareil à une heure de moindre consommation. Par ailleurs, Nokia développe actuellement des services d'aide au maintien au domicile des personnes dépendantes : dans ce cadre, les puces permettront d'obtenir des informations sur l'usage d'un traitement ou l'observance d'un traitement médicamenteux.

Mais, si les différents usages des puces *RFID* visent à apporter de nouvelles facilités aux utilisateurs (badge d'accès à une voiture, un parking, étiquettes sur un produit alimentaire qui permettront bientôt à un réfrigérateur de

lire les dates de péremption…), ils sont également porteurs de risques nouveaux au regard du droit à la vie privée.

En premier lieu, les puces *RFID*, qui contiennent des données personnelles et racontent à ce titre une partie de la vie privée d'un individu, peuvent être interrogées à distance. Il est donc indispensable qu'elles restent sous notre entier contrôle et qu'elles ne parlent pas de nous-même sans notre consentement. L'enjeu est de taille, car les puces *RFID*, qui permettront une identification unique et une traçabilité complète d'un objet, peuvent survivre à cinq générations d'utilisateurs. Fort de ce constat, le Conseil des ministres Télécoms du 27 novembre 2008, sous l'impulsion de la présidence française de l'Union européenne, a reconnu un « droit au silence des puces ».

Ce droit, proposé par la France à ses partenaires européens, a été accepté comme un principe de base de l'action de l'Union européenne dans ce domaine. À l'origine, le droit européen prévoyait qu'à la sortie des supermarchés, les puces apposées sur les produits restaient activées, à charge pour le consommateur de les désactiver. Le droit au silence des puces s'oppose à cette pratique et impose que les puces soient désactivées d'office. La démarche du consommateur doit désormais être de les activer, donc d'exprimer son consentement.

Pour être pleinement effectif, ce droit au silence des puces nécessite que les entreprises manufacturières produisent en amont des puces qui soient désactivables à tout moment. Dans cette perspective, la Commission européenne a publié, en mai 2009, une recommandation sur la mise en œuvre des principes de respect de la vie privée et de protection des données dont les applications reposent sur l'identification par radiofréquence. Elle prévoit que les États membres assurent la collaboration entre les entreprises et les parties intéressées de la société civile en vue de parvenir à l'élaboration d'un cadre d'évaluation de leur impact sur la protection des données.

En deuxième lieu, parce que ces puces *RFID*, qui peuvent être interrogées à distance, contiennent des données à caractère personnel, il est indispensable d'interdire à des tiers non autorisés l'accès à ces informations.

Enfin, compte tenu de la miniaturisation des puces *RFID*, il convient de les rendre visibles et de signaler clairement leur présence par un son, une lumière ou un signal lorsqu'elles sont activées. Il s'agit là d'une proposition faite en octobre 2008 par l'*Electronic Privacy Information Center*, principale association américaine de protection des données personnelles, dont la mission a rencontré les représentants lors de son déplacement à Washington [(1)].

(1) Déplacement à Washington du 1er au 4 février 2011.

Orientation n° 17 : intégrer dans l'usage des puces *RFID* le respect de la vie privée

Renforcer la protection de la vie privée dans le cadre de l'utilisation des puces *RFID* :

— en interdisant à des tiers non autorisés l'accès aux informations qu'elles contiennent ;

— en rendant visibles leur présence par un son, une lumière ou un signal lorsqu'elles sont activées.

6. La vie privée entre profils et profits : le ciblage publicitaire en question

Si le Web 2.0 offre à l'internaute nombre d'applications et de services gratuits, comme les moteurs de recherche ou les réseaux sociaux, c'est en contrepartie d'une offre publicitaire qui ne le lâche jamais lorsqu'il navigue sur Internet et qui le cible au plus près de ses attentes et de ses besoins. Cette contrepartie n'est pas mince, puisque les revenus publicitaires sur Internet aux États-Unis ont augmenté de 15 % en 2010 pour atteindre 26 milliards de dollars, un niveau sans précédent qui témoigne de l'intérêt croissant des entreprises pour la publicité en ligne. En France, la publicité en ligne rapporte en moyenne, chaque année, 3,5 milliards d'euros.

La « Toile » a fait aujourd'hui tellement de progrès que les sites les plus importants peuvent fournir des publicités fondées sur l'historique des recherches effectuées par les internautes. Par exemple, *Google* offre des messages publicitaires à ses utilisateurs au moment où ils sont en quête d'informations sur Internet, c'est-à-dire le moment où ils sont le plus vulnérables. De la même manière, comme l'a rappelé le rapport de M. Yves Détraigne et Mme Anne-Marie Escoffier, le service de messagerie électronique gratuit de *Google*, *Gmail*, est financé par les publicités affichées en fonction du repérage d'un certain nombre de mots-clés figurant dans le contenu des correspondances échangées.

Sur le site *Amazon,* spécialisé dans les ventes de livres*,* chaque consommateur fait l'objet, depuis de nombreuses années, de propositions d'achats personnalisées en fonction du type d'ouvrage qu'il préfère. La société *Apple* est, pour sa part, en train d'entrer sur le marché de la publicité ciblée en utilisant les données accumulées pendant des années sur les préférences musicales des jeunes et les achats de logiciels.

La société *Yahoo !* n'est pas épargnée par la publicité ciblée, qu'elle a été amenée à développer en France en 2007 en vue de permettre aux marques d'atteindre le bon consommateur, au bon moment, en fonction des informations laissées par l'internaute sur les sites de *Yahoo !* Ces données peuvent être recueillies à partir des pages visitées des sites *Yahoo !*, des mots-clés utilisés dans un moteur de recherche *Yahoo !* et des publicités sur lesquelles les internautes

cliquent. Le profil de l'utilisateur qui s'en dégage permet de définir ses intérêts et d'évaluer ses intentions d'achat.

Si la publicité en ligne présente des formes variées, il est possible, à partir de l'étude réalisée par la CNIL sur le ciblage publicitaire [(1)], d'identifier trois types de publicité ciblée sur Internet.

Il s'agit, en premier lieu, de la *publicité personnalisée dite « classique »*. Elle cible l'internaute en fonction d'informations (âge, sexe, localisation, etc.) qu'il a lui-même renseignées. Ce type de publicité est aujourd'hui également utilisé par les réseaux sociaux en fonction des informations (qui peuvent être particulièrement nombreuses) fournies par leurs utilisateurs dans leurs « profils ».

Il s'agit, en deuxième lieu, de la *publicité contextuelle*. Elle cible l'internaute en fonction des contenus immédiatement consultés ou, dans le cas d'un moteur de recherche, sollicités (contenu contextuel de la page consultée, relation avec le ou les mots-clés saisi(s) sur un moteur de recherche, etc.). Elle permet également de cibler l'internaute en fonction de l'endroit où il se trouve, ces informations de géolocalisation étant déduites de son adresse IP (pays ou région d'origine, langue utilisée).

La troisième forme de publicité ciblée, qui est aussi la plus élaborée à ce jour, est la *publicité comportementale* fondée sur l'observation du comportement de l'internaute à travers le temps. À partir des différents sites qu'il a consultés, des mots-clés qu'il a saisis et des contenus qu'il a produits, elle établit un profil de l'internaute et peut ainsi lui proposer des publicités adaptées à son profil. Parmi les différentes techniques permettant de constituer de tels profils, la plus connue et la plus employée est celle des « *cookies* », témoins de connexion qui s'installent le plus souvent à l'insu de l'internaute sur son ordinateur personnel.

Ces trois formes de publicités, si elles empruntent des voies différentes, poursuivent toutes un même objectif que M. Carlo d'Asaro Biondo, directeur de *Google France*, a résumé en ces termes dans une interview accordée à la *Tribune* en juin 2010 : « *Comprendre ce que recherche tel type de personnes à tel moment dans telle région permet d'apporter aux internautes des publicités qui correspondent davantage à leurs recherches. Cela diminue la déperdition pour les annonceurs et augmente la valeur de la publicité. Quand les médias refusent de faire évoluer la publicité au nom de ces données personnelles, ils se tirent une balle dans le pied* ».

Comme l'ont souligné M. Yves Détraigne et Mme Anne-Marie Escoffier, les acteurs de la publicité en ligne « *se défendent de participer à l'instauration d'une société de surveillance dans la mesure où, font-ils valoir, la collecte de ces informations demeure anonyme : le but n'est pas d'épier les comportements d'utilisateurs identifiés mais de parvenir à une « personnalisation » des services*

(1) « La publicité ciblée en ligne *», communication présentée par M. Bernard Peyrat, rapporteur, en séance plénière le 5 février 2009.*

proposés, au double bénéfice de l'internaute et de l'annonceur publicitaire ». Cette thèse a également été soutenue devant la mission. M. Justin Weiss, directeur de la politique internationale en matière de données personnelles de *Yahoo !*, a ainsi rappelé que l'intérêt des acteurs de l'Internet était de faire un usage limité des informations disponibles. Dans cette perspective, le ciblage publicitaire conduit à restreindre le champ des données pertinentes et à ne pas prendre en compte les données proprement personnelles utilisées pour l'ouverture des comptes.

En effet, le ciblage est basé sur le nombre de clics effectués sur les pages ayant un contenu pertinent – par exemple cliquer sur un contenu se rapportant au sport peut représenter une donnée. Les clics sont enregistrés dans des fichiers – les *logfiles* (1) – définissant un profil de l'utilisateur. Les autres sources de données sont les termes utilisés par l'internaute dans les moteurs de recherche ainsi que l'accès à des sites de publicité, que celle-ci soit ciblée ou non. Rassemblées dans des *logs*, ces données sont utilisées pour que l'utilisateur reçoive des publicités correspondant à ses intérêts. Si les paramètres de ciblage sont modifiés ou bloqués, les publicités parviendront toujours à l'internaute, mais leur contenu ne prendra pas en compte les navigations auxquelles l'utilisateur aura procédé.

M. Justin Weiss a insisté sur la distinction qu'il convenait de faire entre ces données et celles qui sont déclarées pour ouvrir un compte *Yahoo !*. Ces dernières ne sont pas nécessaires au ciblage. Aussi précises que soient les données utilisées pour le ciblage, celles-ci ne s'identifieraient donc pas avec les données personnelles de l'internaute. Il s'agit de deux systèmes différents. La preuve en serait que font l'objet d'un ciblage aussi bien les personnes inscrites sur *Yahoo !* que celles qui n'ont pas de compte et ne font que consulter les sites.

Les sociétés développant un service de publicité ciblée se sont également efforcées dans leurs activités de respecter la vie privée et les données personnelles des internautes.

Ainsi, quand *Yahoo !* a introduit son système de publicité ciblée, les conditions générales d'utilisation, y compris les conditions de conservation des données personnelles, ont été adaptées pour que l'utilisateur soit informé de la nature des données conservées, de leur utilisation et surtout du contrôle qu'il a sur elles. Ce contrôle s'effectue de la manière suivante : au bas de chaque page ouverte sur *Yahoo !,* se trouve un lien qui permet d'ouvrir une page de données personnelles ; sur cette page, est proposée à l'internaute une fonction de gestion des publicités basées sur ses centres d'intérêt, définis en fonction de ses données de navigation sur le réseau. Si, selon le principe de *l'opt out*, l'internaute ouvre cette page, il peut modifier, désélectionner ou bloquer l'ensemble des centres d'intérêt. Le contrôle est donc soit granulaire, catégorie par catégorie, soit global. L'utilisateur bénéficie de la même transparence pour les données portant sur le sexe, sa tranche d'âge ou son adresse IP. La transparence en matière de ciblage

(1) Fichier journal qui enregistre les événements se produisant dans un système informatique.

consiste pour *Yahoo !* à porter à la connaissance de l'internaute non seulement les catégories d'information servant à établir les profils mais aussi à indiquer les types de données utilisées à cette fin.

Cependant, faute de transparence et d'information préalable, l'internaute peut vivre la publicité ciblée dont il fait l'objet comme une forme d'intrusion dans sa vie privée. En effet, comme l'a montré la CNIL dans son étude précitée, « *en l'absence de transparence de la part des fournisseurs de contenu ou de services sur les mécanismes de profilage et sur les données collectées, l'internaute peut percevoir ces mécanismes comme très intrusifs* » (1).

Face à ces difficultés, l'Europe s'est emparée de la question du ciblage publicitaire, lors de l'adoption du « Paquet Télécoms », à l'automne 2009. Ainsi, la directive 2009/136/CE du 25 novembre 2009, dont la portée a été explicitée par un avis G29 du 22 juin 2010 (cf. *infra*), autorise les traitements de données réalisés par les opérateurs dans un but commercial si les abonnés y consentent expressément et pour une durée déterminée. Elle fait également obligation aux opérateurs d'informer de manière claire et complète l'utilisateur et d'obtenir son accord avant d'installer des *cookies*.

L'AVIS DU GROUPE DES « CNIL » EUROPÉENNES DU 22 JUIN 2010

Le G29, le groupe des CNIL européennes, a adopté le 22 juin 2010 un avis sur la publicité comportementale en ligne, notamment au regard des dispositions européennes, et, en particulier de la directive 2002/58/CE « vie privée et communications électroniques » révisée par la directive 2009/136/CE du 25 novembre 2009. Cet avis souligne que :

— l'article 5-3 de la nouvelle directive « vie privée et communications électroniques » impose un consentement explicite et préalable de la personne concernée. Celle-ci doit donc donner son accord pour l'envoi de *cookies* et le suivi ultérieur de son comportement de navigation pour lui adresser des annonces personnalisées.

— les régies publicitaires (par exemple, celles des sociétés *Google*, Microsoft et *Yahoo*) sont responsables de traitement dans la mesure où ce sont elles qui déterminent les finalités et les moyens essentiels de ce traitement des données.

— les éditeurs, c'est-à-dire les sites où sont affichés les bandeaux publicitaires, assument également une part de la responsabilité incombant au responsable du traitement. En configurant leurs sites web, ils déclenchent le transfert de l'adresse IP de l'utilisateur vers les fournisseurs de réseaux publicitaires.

— les régies publicitaires et les éditeurs sont donc tenus de donner aux internautes, préalablement à toute collecte de données sur leur comportement, une information claire et transparente sur les informations collectées et la constitution de profils, la diffusion d'annonces ciblées.

— l'industrie de la publicité en ligne (régies et éditeurs) doit donc développer rapidement des outils faciles à utiliser pour les internautes, pour mettre en œuvre ces principes de protection de la vie privée.

L'avis du G29 reprend donc largement celui de la CNIL de février 2009 en décrivant les obligations découlant des modifications de la directive 2002/58/CE « vie privée et communications électroniques », qui doit être transposée dans notre droit national avant le 25 mai 2011.

Source : www.cnil.fr

(1) « La publicité ciblée en ligne *»,* op. cit.*, p. 22.*

En l'état actuel, la loi n° 78-17 du 6 janvier 1978 dite « loi Informatique et libertés » reconnaît, à son article 38, un droit d'opposition à l'utilisation de ses données personnelles à des fins commerciales, toute personne physique ayant « *le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur* ».

Autre facteur d'optimisme en matière de publicité ciblée : lors de son audition par la mission [(1)], M. Alex Türk, président de la CNIL, avait indiqué que les systèmes de publicité ciblée que l'autorité administrative qu'ils président avait eu à examiner garantissaient tous la préservation de l'anonymat. Ils ne posent donc pas, à ses yeux, de difficulté juridique.

Il convient enfin de signaler l'action entreprise par les pouvoirs publics afin de responsabiliser les acteurs de la publicité ciblée. Le 30 septembre 2010, la secrétaire d'État chargée de la prospective et du développement de l'économie numérique, Mme Nathalie Kosciusko-Morizet, a signé avec dix acteurs du monde numérique [(2)] une charte sur la publicité ciblée et la protection des internautes. Cette charte comprend huit engagements, qui vont permettre aux internautes d'être mieux informés sur les pratiques des régies publicitaires.

Ainsi, les associations professionnelles s'engagent à indiquer de manière claire [(3)] la nature et le moyen de collecte des données utilisées à des fins commerciales et à mettre en évidence les méthodes de suppression ou de refus des *cookies*. Le tout dans un langage clair, qui pourrait adopter la forme de schémas ou de questions-réponses.

Les régies publicitaires se sont également engagées à créer une plate-forme qui permettra aux internautes d'accepter ou de refuser l'affichage de publicités ciblées. Les utilisateurs de mobiles devraient aussi se voir proposer de manière claire le droit d'accepter ou de refuser que leur terminal fasse l'objet d'une localisation dans le but d'afficher des publicités géolocalisées.

Les professionnels du secteur s'engagent également à restreindre dans le temps l'usage des *cookies* publicitaires : par défaut leur durée de vie serait fixée à 60 jours. Cependant, ils se réservent le droit d'appliquer des durées plus longues ou plus courtes « proportionnées à la durée de cycle d'achat des produits ou services promus ».

Les associations professionnelles se sont enfin mises d'accord sur la mise en place des dispositifs de protection, notamment envers les jeunes internautes Ils

(1) Audition du 19 mai 2010.

(2) Association des Agences Conseil en Communication, Fédération e-commerce et vente à distance, Groupement des éditeurs de services en ligne, Internet Advertising Bureau France, Mobile Marketing Association France, Syndicat National de la Communication Directe, Syndicat des Régies Internet, Union des Annonceurs, Union Des Entreprises de Conseil et Achat Media, Union Française du Marketing Direct.

(3) Sous forme de schémas ou de questions-réponses.

se sont ainsi engagés à ne créer aucune catégorie recensant les comportements et centres d'intérêt des moins de 13 ans.

II. LE RESPECT DE LA VIE PRIVÉE : UNE PROTECTION ET UN CADRE JURIDIQUE À RENOUVELER

Comme la mission vient de le démontrer, les récents progrès technologiques ont suscité de nouveaux usages qui, au-delà de l'attrait qu'ils peuvent susciter, sont susceptibles de porter atteinte au respect de la vie privée. C'est aux États en général et aux législateurs en particulier qu'il revient dès aujourd'hui d'apporter des réponses à tous les niveaux – national, européen et international – afin non pas de faire évoluer notre conception de la vie privée au fil des innovations technologiques, mais, bien au contraire, de préserver nos libertés individuelles, en adaptant pour ce faire les nouvelles technologies à notre conception de la vie privée.

A. ADAPTER LE CADRE JURIDIQUE NATIONAL AUX RÉCENTS PROGRÈS TECHNOLOGIQUES

La maîtrise du développement technologique dans le respect de notre vision de la vie privée exige tout d'abord que des solutions soient définies au niveau national. Si la loi « Informatique et libertés » du 6 janvier 1978 demeure le socle fondateur de la protection de la vie privée en France, elle doit cependant être adaptée afin de répondre à trois enjeux : le statut de l'adresse IP, le droit à l'oubli et le consentement de l'internaute.

1. Le socle fondateur de la protection de la vie privée : la loi du 6 janvier 1978

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés demeure aujourd'hui une loi fondatrice, pierre angulaire de la protection des citoyens face aux traitements de données à caractère personnel. Il s'agit d'un cadre juridique pionnier qui a devancé et inspiré la mise en place de règles aux niveaux international et européen. Elle fut modifiée une seule fois, en 2004, afin de transposer la directive européenne du 24 octobre 1995.

L'objectif poursuivi par la loi *Informatique et liberté* du 6 janvier 1978 est, comme le rappelle son article premier, de mettre l'informatique au service de chaque citoyen, son développement devant s'opérer dans le cadre de la coopération internationale sans toutefois « *porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Cette loi soumet la création et l'utilisation des traitements de données à caractère personnel au respect de trois principes majeurs.

En premier lieu, la collecte, la consultation ou la transmission de données personnelles doivent répondre au principe de finalité, consacré à l'article 6 de la loi du 6 février 1978 qui dispose que les données à caractère personnel « *sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* ». Le non-respect de ce principe est sanctionné par l'article 226-21 du code pénal qui prévoit que l'utilisation d'un traitement à d'autres fins que celles définies lors de sa création est constitutive d'un délit puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

En deuxième lieu, l'enregistrement et l'utilisation des données personnelles doivent également obéir au principe de proportionnalité, qui, bien que ne figurant pas expressément dans la loi du 6 janvier 1978, inspire sans conteste son article 6 qui prévoit que les données à caractère personnel doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » et ne peuvent être conservées que « *pendant une durée (n'excédant) pas la durée nécessaire aux finalités* ».

En troisième et dernier lieu, les responsables de traitements de données à caractère personnel doivent, au nom du principe de sécurité énoncé à l'article 34 de la loi du 6 février 1978 « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». Le respect de ce principe de sécurité est sanctionné par l'article 226-17 du code pénal qui dispose que le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans respecter les mesures prescrites en matière de sécurité des données est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Si le responsable d'un traitement de données personnelles se voit soumis à de multiples impératifs – comme le respect des principes de finalité, de proportionnalité et de sécurité –, les personnes qui voient leurs données ainsi collectées bénéficient, en contrepartie, de quatre grands droits.

En premier lieu, elles bénéficient d'un droit d'accès et de rectification de leurs données personnelles. En application des articles 39 à 43 de la loi du 6 janvier 1978, « *toute personne physique justifiant de son identité [a le droit] d'interroger le responsable d'un traitement de données à caractère personnel* » [(1)] et d'« *exiger [de lui] que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite* » [(2)].

(1) Article 39 de la loi du 6 janvier 1978.
(2) Article 40 de la loi du 6 janvier 1978.

En deuxième lieu, en cas de collecte de données personnelles directement auprès de la personne concernée, celle-ci doit être informée entre autres de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant, de la finalité poursuivie par le traitement auquel les données sont destinées, des destinataires ou catégories de destinataires des données et des droits – notamment d'accès et de rectification – dont elle bénéficie. Il s'agit du droit d'information prévu à l'article 32 de loi du 6 janvier 1978 : les fichiers ne doivent pas être créés à l'insu des personnes concernées et les responsables de traitements de données ne peuvent les laisser dans l'ignorance sur ce qu'ils vont faire de ces données. En cas de collecte indirecte de ces données, ce droit à l'information existe, le responsable du traitement pouvant cependant s'en exonérer si cette information « *se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche* ».

En troisième lieu, toute personne « *a le droit de s'opposer, pour des raisons légitimes, à ce que des données la concernant fassent l'objet d'un traitement* ». Il s'agit du droit d'opposition à ses données personnelles, proclamé à l'article 38 de la loi du 6 janvier 1978. L'exercice de ce droit est soumis à l'existence de « *raisons légitimes* », qui correspondent à des motifs tenant à une situation particulière et l'emportant sur les intérêts du responsable de traitement. En cas de litige, le juge tranche et apprécie très souplement l'existence de ces raisons légitimes, dans le sens de la protection des individus. Ce droit d'opposition peut s'exercer, par une demande expresse, lors de la collecte ou ultérieurement, en demandant notamment la suppression des données conservées.

En quatrième et dernier lieu, la loi précitée du 6 août 2004 a consacré à l'article 7 de la loi du 6 janvier 1978 un nouveau droit, celui au consentement préalable, aux termes duquel « *un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée* ». Le responsable de traitement peut toutefois s'affranchir du consentement dans de très nombreux cas, de sorte que le régime applicable est essentiellement celui du droit d'opposition précité.

La loi du 6 janvier 1978, qui n'a connu en plus de trente ans qu'une seule modification d'ampleur, a montré son efficacité et son adaptabilité aux diverses évolutions technologiques qui n'ont cessé de se multiplier ces dernières. Les principes qui la régissent ont, comme le rappellent dans leur rapport M. Yves Détraigne et Mme Anne-Marie Escoffier, se sont révélés, grâce à leur « *modernité* » et à leur « *extrême plasticité* », « *applicables et adaptés à l'ensemble des nouvelles technologies numériques qu'elles aient pour effet principal ou incident de collecter des données permettant de tracer un individu dans le temps et l'espace* » (1).

La loi *Informatique et libertés* semble ainsi avoir rempli l'objectif qui lui avait été assigné et que le rapporteur du projet de loi au Sénat, M. Jacques

(1) Rapport d'information n° 441, op. cit*, p. 40.*

Thyraud, avait résumé en ces termes : « *la tâche du législateur consiste à faire des lois les plus générales et les plus claires possible afin de permettre, dans l'application, une certaine souplesse. Cette exigence est d'autant plus forte que le secteur auquel s'applique la loi est plus technique et évolutif* ».

Si la loi du 6 janvier 1978 a su poser les bases juridiques garantissant de manière satisfaisante et équilibrée la protection des données personnelles, de nombreuses questions subsistent et auxquelles il convient d'apporter une réponse.

2. L'identité de l'internaute : le statut de l'adresse IP en question

La première question à laquelle la mission a été confrontée lors de ses auditions est celle du statut de l'adresse IP [(1)]. Si cette question avait fait l'objet de vifs débats lors de l'examen des projets de loi favorisant la diffusion et la protection de la création sur Internet, elle n'avait toutefois pas trouvé de solution.

QU'EST-CE QU'UNE ADRESSE IP ?

Sur Internet, les ordinateurs communiquent entre eux grâce au Protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresses IP. Dans sa version 4, ces adresses sont composées de quatre nombres entiers compris chacun entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Chaque ordinateur relié à un réseau dispose d'une adresse IP unique, ce qui lui permet de communiquer avec les autres ordinateurs du même réseau. De même, chaque site Internet dispose d'une adresse IP, qui peut être convertie en nom de domaine. L'attribution des adresses IP publiques relève de l'ICANN *(Internet Corporation for Assigned Names and Numbers*).

Concrètement, chaque transmission de données sur le web donne lieu à l'envoi d'un « *paquet de données* » comprenant, quel que soit le type de communication (navigation sur le web, messagerie, téléphonie par Internet, *etc.*) l'adresse IP de l'expéditeur ainsi que celle du destinataire. Ainsi, lorsqu'un internaute consulte un site Internet, le serveur de ce dernier enregistre dans un fichier la date, l'heure et l'adresse IP de l'ordinateur à partir duquel la consultation a été effectuée, ainsi que les fichiers qui ont pu être envoyés. Le propriétaire du site a ainsi accès aux adresses IP des ordinateurs qui se sont connectés à son site.

Source : rapport d'information n° 441, op. cit.*, p. 57.*

L'adresse IP est-elle une donnée à caractère personnel au sens de l'article 2 de la loi du 6 janvier 1978, à savoir une information « *relative à une personne identifiée ou identifiable* » ? La réponse à cette question nécessite au préalable de savoir s'il est possible techniquement d'identifier un individu précis à partir de la seule adresse IP.

Lors de leur audition par la mission [(2)], MM. Thomas Clausen et Fabrice Le Fessant, qui enseignant à l'École polytechnique*,* ont indiqué que, sur un plan technique, l'adresse IP ne permettait pas, la plupart du temps et avec certitude, d'identifier directement un internaute. Plusieurs raisons peuvent être avancées pour expliquer une telle situation.

(1) Une adresse IP (Internet Protocol) est un numéro qui identifie l'interface avec le réseau Internet de tout matériel informatique.

(2) Audition du 5 mai 2010.

En premier lieu, la même personne qui se connecte depuis des endroits différents a des adresses IP différentes. Il en va de même dans le cas de deux connexions successives au même endroit, dès lors que ces adresses sont attribuées de façon dynamique et temporaire – pour la durée d'une connexion ou d'une journée – par un fournisseur d'accès. L'adresse est certes, à un moment donné, unique, mais elle peut varier au cours du temps pour un même individu.

En second lieu, s'il s'agit d'une adresse IP privée à laquelle on se connecte depuis un lieu public – par exemple dans un café –, il n'y a alors aucun moyen d'identifier l'internaute. Il en va de même pour les réseaux privés familiaux. En outre les mécanismes de contrôle d'accès – du type WEP (1) – sur les réseaux sans fil ne sont pas sûrs. Dix minutes suffisent pour « craquer » ce type d'installation et usurper par piratage un réseau Wifi, ce dont les consommateurs ne sont pas conscients.

Or, le problème de l'identification des adresses IP risque de se généraliser non seulement du fait des usurpations d'adresses mais pour des raisons simplement techniques. Gérées par un organisme situé aux États-Unis, les adresses IP sont en effet en nombre limité. Fin 2010, aucune nouvelle adresse ne devait pouvoir être attribuée, faute d'adresses IP V4 disponibles. En attendant l'introduction du nouveau format V6 (2), des technologies existent pour remédier provisoirement à cette pénurie d'adresses.

Un procédé consiste en particulier à utiliser une adresse IP identique pour un groupe d'utilisateurs, le titulaire de l'adresse servant d'intermédiaire pour les requêtes des autres. Ce système est en place à l'École polytechnique où tous les élèves se connectent sous la même adresse. Pour l'extérieur, l'ensemble des utilisateurs apparaît alors comme une seule entité. Ce système est utilisé dans de nombreuses institutions et peut l'être aussi dans un cadre plus familial, la technologie étant facilement abordable. Quand il sera recouru à cette technologie non seulement à la demande du client mais à l'initiative du fournisseur d'accès - lequel attribuera par exemple une identité unique à toute une ville – il deviendra de plus en plus difficile d'identifier le trafic de données de tel ou tel internaute.

Pour M. Thomas Clausen, l'identification d'un accès à Internet à partir de l'adresse IP est possible pour autant que l'internaute est client d'un fournisseur d'accès et que celui-ci peut établir qu'il y a eu telle connexion à tel moment. Mais dans le cas où, en raison d'une pénurie d'adresses, le fournisseur n'est pas en mesure de donner une adresse pour chacun de ses clients, cela devient plus difficile. Il faudra pour ce faire attendre le développement des IP V6, qui nécessite du temps.

Lors de son audition par vos rapporteurs (3), M. Maxime Lombardini, directeur général d'Iliad Free, a souligné les mêmes difficultés d'identification de

(1) WEP : Wired Equivalent Privacy, protocole de sécurisation des réseaux sans fil.
(2) Ce nouveau format permettra de disposer de 3,4 × 1038 adresses.
(3) Audition du 8 juin 2010.

l'internaute à partir de l'adresse IP. En effet, celle-ci appartient à un abonné tant qu'il est chez l'opérateur mais peut être par la suite affectée à un autre abonné. Il s'agit donc d'une donnée complexe à suivre dans le temps. Il avait ainsi évoqué l'histoire d'une famille ayant été perquisitionnée brutalement pour une affaire de pédophilie sur le net qui concernait un abonné ayant quitté Free une semaine auparavant.

L'adresse IP n'est donc pas un moyen fiable et efficace pour identifier les internautes et il ne semble pas exister de technique spécifique qui rendrait possible une telle identification. Faut-il pour autant dans ces conditions renoncer définitivement à considérer l'adresse IP comme une donnée à caractère personnelle ? Les jurisprudences nationale et européenne apportent à cet égard un début de réponse.

Compte tenu des contraintes techniques qui viennent d'être évoquées, le juge judiciaire français a estimé que l'adresse IP ne pouvait pas être considérée comme une donnée personnelle, dans la mesure où « *elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon* » (1) ne permettant « *pas d'identifier le ou les personnes qui ont utilisé cet ordinateur* » (2)

Ni le juge administratif français (3), ni le juge européen (4) n'a suivi cette position, puisqu'ils ont, pour leur part, considéré que l'adresse IP était une donnée personnelle garantie et protégée par la loi du 6 janvier 1978 comme par la directive du 24 octobre 1995. Cette jurisprudence est conforme, d'une part, à l'avis rendu par le G29 (5), le 20 juin 2007, dans lequel il rappelle que l'adresse IP attribuée à un internaute lors de ses communications doit être regardée comme une donnée à caractère personnel, ainsi que, d'autre part, à l'article 2 de la directive du 15 mars 2006 qui dispose désormais que les données à caractère personnel comprennent les données relatives au trafic et les données de localisation ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur, incluant à ce titre l'adresse IP.

Face à cette situation marquée par des évolutions techniques à venir et un cadre juridique qui reste à stabiliser, la mission juge important que la protection des données personnelles liées à l'adresse IP soit assurée, une telle protection passant par une clarification du statut juridique de l'adresse IP.

Orientation n° 18 : clarifier le statut juridique de l'adresse IP pour renforcer la protection des données personnelles qui lui sont liées

(1) Cour d'appel de Paris, 13e chambre, 15 mai 2007.
(2) Cour d'appel de Paris, 13e chambre, 27 avril 2007.
(3) CE, 23 mai 2007, SACEM et autres*.*
(4) CJCE, 29 janvier 2008, Promusicae*, dans une affaire relative à la lutte contre le piratage.*
(5) Groupe de travail Article 29 sur la protection des données.

Au-delà du statut juridique de l'adresse IP, se pose la question de l'anonymisation et de la suppression des personnelles liées à cette adresse. En mai 2010, le G29 a officiellement écrit aux trois géants de l'Internet, *Google*, *Microsoft* et *Yahoo*, pour leur suggérer de rapidement vérifier la façon dont ils préservent l'anonymat des internautes. Était en cause la durée de conservation des recherches effectuées sur les trois moteurs, qui restent liées à l'adresse IP des ordinateurs des internautes et permettent de les identifier, d'obtenir des éléments sur leurs goûts, leurs comportements, éléments qui sont ensuite commercialisés à des annonceurs.

En effet, la durée de conservation des données personnelles liées à l'adresse IP et communiquées à l'occasion de recherches sur Internet est variable : 9 mois pour *Google*, 3 mois pour *Yahoo !* Microsoft a décidé de suivre les recommandations du G29 en détruisant, après 6 mois de conservation, les références aux adresses IP des utilisateurs de ses services. Microsoft procède également à une anonymisation complète de ces données, « jusqu'au dernier octet » pour rendre impossible toute reconstitution de l'adresse par rétro-ingénierie. Une telle demande est formulée par de nombreuses associations, notamment par l'*Electronic Privacy Information Center* (EPIC) aux États-Unis.

La mission considère qu'il est essentiel que les recommandations du G29 soient mises en œuvre sans délai par les fournisseurs de services, auxquels il revient, d'une part, de détruire, après six mois de conservation, les données personnelles liées aux adresses IP des utilisateurs de ses services et, d'autre part, d'anonymiser complètement ces données, jusqu'au dernier octet, pour rendre impossible toute reconstitution de l'adresse par rétro-ingénierie.

Orientation n° 19 : pour une destruction et une anonymisation complètes des données par les fournisseurs de services après six mois

Contraindre les fournisseurs de services, conformément aux recommandations du G29, d'une part, à détruire, après six mois de conservation, les références aux adresses IP des utilisateurs de ses services et, d'autre part, à anonymiser complètement ces données, jusqu'au dernier octet, pour rendre impossible toute reconstitution de l'adresse par rétro-ingénierie.

3. Le droit à l'oubli : retour sur une idée séduisante, mais peu opérante

À côté du débat sur le statut de l'adresse IP, la mission a, à chacune de ses auditions, dû faire face à la question récurrente et sur lesquels les avis sont très partagés, celle du droit à l'oubli.

En effet, les facilités apportées par certaines nouvelles technologies, au nombre desquelles figurent les moteurs de recherche comme *Google*, Bing ou *Yahoo !*, peuvent pousser les individus, par ignorance ou par indifférence, à mettre de côté la protection de leur vie privée et à exposer volontairement, par le biais de

blogs ou de réseaux sociaux (tels que *Facebook*, *MySpace*, etc.), des pans entiers de leur vie privée sur Internet.

Si la collecte et la conservation de données personnelles ne sont pas par principe condamnables et s'avèrent le plus souvent utiles, elles doivent néanmoins être assorties de garanties afin de respecter la vie privée de nos concitoyens.

On a vu que la législation française reconnaissait d'ores et déjà quatre droits en matière de conservation des données :

- le droit pour toute personne d'accéder à l'intégralité des données conservées à son sujet [(1)] ;
- le droit pour toute personne d'être informée de la mise en œuvre d'un traitement de données personnelles [(2)] ;
- le droit pour toute personne de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et de refuser, sans avoir à se justifier, que les données la concernant soient utilisées à des fins de prospection commerciale [(3)] ;
- et, enfin, le droit pour toute personne de faire rectifier, compléter, actualiser ou effacer des informations la concernant lorsqu'ont été décelées des erreurs ou des inexactitudes [(4)].

Mais, avec Internet et les nouvelles technologies, les capacités de conservation des données se sont démultipliées, les informations restant visibles de façon permanente, comme gravée dans le marbre. Se pose donc la question de la reconnaissance d'un véritable droit à l'oubli qui permettrait à toute personne de retirer de « la toile » des informations publiques la concernant et dont elle ne souhaite plus permettre la consultation. Lors de son audition par la mission [(5)], M. Pierre Bellanger a indiqué qu'Internet avait institué un « éternel présent », l'individu risquant, selon le sociologue Dominique Wolton [(6)], d'étouffer sous la mémoire.

Face à ces risques, le droit à l'oubli est régulièrement invoqué. Mais que recouvre en réalité cette notion ?

Le droit à l'oubli est au croisement de trois préoccupations. En premier lieu, les individus souhaitent avoir l'assurance que les données à caractère personnel collectées par une entreprise ou par une administration pour une finalité définie ne seront pas conservées au-delà de la période strictement nécessaire pour atteindre cette finalité. Ils veulent, dans un deuxième temps, avoir la possibilité

(1) Article 39 de la loi n° 78-17 du 6 janvier 1978.
(2) Article 32 de la loi n° 78-17 du 6 janvier 1978.
(3) Article 38 de la loi n° 78-17 du 6 janvier 1978.
(4) Article 40 de la loi n° 78-17 du 6 janvier 1978.
(5) Audition du 14 septembre 2010.
(6) Audition du 30 juin 2010.

d'effacer les informations qu'ils ont mises en ligne sur une plateforme de partage, comme *Facebook*, lorsqu'il décide de retirer de leurs profils les informations les concernant. Ils veulent enfin avoir l'assurance que les informations qu'eux-mêmes ou un tiers ont rendues publiques et disponibles sur Internet puissent ne pas être facilement accessibles au-delà d'un certain délai.

Ainsi défini, les pouvoirs publics ont cherché à faciliter l'accès d'un tel droit. Ainsi, la secrétaire d'État chargée de la prospective et du développement de l'économie numérique, Mme Nathalie Kosciusko-Morizet, a signé avec dix acteurs du monde numérique une charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche visant à garantir aux internautes le respect de leur vie privée en leur permettant de mieux contrôler la publication des données les concernant.

CHARTE DU DROIT À L'OUBLI DANS LES SITES COLLABORATIFS ET LES MOTEURS DE RECHERCHE DU 13 OCTOBRE 2010

Les dix acteurs signataires – Action innocence, Confédération nationale des associations familiales catholiques, *e*-enfance, Union nationale des associations familiales, Copains d'avant, Pages jaunes, Skyrock, Trombi.com, Viadéo, Microsoft France – se sont engagés :

● à améliorer la transparence de l'exploitation des données publiées par les internautes, en fournissant, dès la page d'accueil « *une information conviviale et facilement accessible sur la politique de protection de la vie privée (conditions générales d'utilisation, droits des utilisateurs, utilisation des outils pour régler les paramètres de confidentialité…)* » ;

● à faciliter la possibilité pour une personne de gérer ses données sur la toile, en indiquant, lors de la collecte des données, la durée de conservation des données à caractère personnel, les modalités d'exercice du droit d'opposition, et les conditions d'indexation par les moteurs de recherche ;

● à offrir à l'internaute la possibilité de supprimer ou modifier les données qu'il a publiées via un « bureau de réclamations » virtuel, de visualiser l'ensemble de ses informations personnelles, supprimer son compte grâce à des interfaces simples et pratiques mises en place par les sites collaboratifs ;

● à demander à l'internaute, s'agissant des sites collaboratifs, l'autorisation de transférer leurs données vers des tiers ou vers des applications extérieures (quiz, jeux…) ;

● à éduquer les internautes et à protéger les mineurs, en systématisant notamment les dispositifs permettant de vérifier si les utilisateurs sont mineurs, afin de les protéger d'éventuelles dérives ;

● à protéger les données personnelles de l'indexation automatique par les moteurs de recherche.

Si cette démarche est intéressante en ce qu'elle permet de sensibiliser l'internaute et les citoyens sur le risque de mettre sur Internet des éléments susceptibles de leur nuire par la suite, à l'occasion d'un entretien d'embauche ou autre, elle n'en demeure pas moins limitée à un double titre. En premier lieu, les deux géants du secteur, *Google* et *Facebook*, ont refusé de signer cette charte du droit à l'oubli numérique. La CNIL elle-même n'a pas signé la charte, protestant du fait que certaines entreprises signataires n'avaient pas de correspondant

informatique et libertés. En second lieu, il ne s'agit que d'une simple charte qui n'a, à ce titre, aucune portée normative contraignante.

Mais, l'ensemble des auditions et déplacements réalisés par la mission l'a convaincue que les limites rencontrées par cette charte sur le droit à l'oubli numérique n'étaient que le reflet de l'impossibilité, tant juridique que pratique, de consacrer un droit général et à absolu à l'oubli sur Internet.

En effet, le droit à l'oubli, qui fait l'objet de fréquentes incantations et qui est souvent présenté comme l'ultime rempart de la protection de la vie privée, est d'ores et déjà garanti en France et en Europe par les dispositions législatives en vigueur, comme l'a indiqué M[e] Winston Maxwell lors de son audition [(1)]. En effet, les droits d'accès, d'information, d'opposition et de rectification tels qu'ils sont consacrés par la loi précitée du 6 janvier 1978 et la directive du 24 octobre 1995 permettent en l'état actuel de répondre aux trois préoccupations que recouvre le droit à l'oubli (cf. *supra*). Rendre plus clair ce droit à l'oubli, c'est rendre plus effectif le droit applicable.

Si, sur le plan juridique, la consécration d'un droit spécifique à l'oubli n'est pas nécessaire, il convient de s'interroger, dans un second temps, sur l'applicabilité technique d'un tel droit. La réponse est une nouvelle fois négative. En effet, lors de son audition par la mission [(2)], M[e] Étienne Drouard, avocat à la cour, s'est interrogé sur la notion même d'oubli et sur celle d'un droit qui lui serait rattaché. Parler d'oubli dans les réseaux constitue, selon lui, une gageure puisqu'un contenu peut être conservé sous une multiplicité de formes. Même si une donnée personnelle – photo, vidéo… – parvient à être effacée sur un site ou sur un réseau social, le problème n'est pas pour autant résolu, dans la mesure cette donnée a pu être dupliquée à l'infini sur le réseau. La mémoire sur le réseau n'a pas de limite. Toute donnée « effacée » peut resurgir si elle a été conservée sur un ordinateur.

Toujours sur un plan juridique, la consécration d'un droit général et absolu à l'oubli numérique s'opposerait de front au modèle de l'économie numérique, que symbolisent notamment *Facebook* et *Google*. En effet, les données personnelles fondent le modèle économique du commerce électronique. Les applications du Web 2.0 n'ont de succès que parce qu'elles sont gratuites. Or leur fonctionnement a un coût. Celui-ci n'est couvert que par la valorisation des données personnelles utilisées par la publicité, en particulier comportementale. La consécration d'un tel droit absolu à l'oubli sur Internet risquerait de rompre le point d'équilibre actuel entre le nécessaire financement de l'économie numérique, dont le dynamisme soutient incontestablement la croissance et l'activité de notre pays, et l'indispensable protection de la vie privée dans la société d'information.

Si, sur les plans juridique et technique, le droit à l'oubli numérique ne saurait exister en tant que tel, il convient cependant, afin de renforcer l'effectivité

(1) Audition du 10 novembre 2010.
(2) Audition du 6 juillet 2010.

des droits d'accès, d'information, d'opposition et de rectification consacrés par les dispositions législatives actuelles, d'améliorer en amont la maîtrise de l'information par l'usager plutôt que chercher à effacer les informations une fois qu'elles sont diffusées sur Internet (cf. *infra*).

Comme l'ont indiqué à la mission les représentants de la société *Google* (1), celle-ci a souhaité aller plus loin dans la mise en place d'outils permettant à l'internaute d'assurer un meilleur contrôle de ses données, à travers la création du « *Dashboard* ». Il s'agit d'un tableau de bord qui permet à l'internaute utilisant les produits *Google* d'être informé sur l'ensemble des données que *Google* conserve sur lui et d'en garder le contrôle. Il peut ainsi retirer des données ou choisir des paramètres de confidentialité. Ce système est applicable à l'ensemble des produits pour lesquels l'internaute possède un compte *Google* : *Gmail*, *YouTube* etc.

Orientation n° 20 : permettre à l'internaute, mieux informé, de contrôler ses données personnelles

Plutôt que de consacrer un droit général et absolu à l'oubli numérique, qui ne serait pas opérationnel, améliorer en amont l'information de l'internaute, en lui offrant des outils lui permettant d'assurer un meilleur contrôle de ses données personnelles.

S'il n'est pas possible, comme la mission vient de l'indiquer, de consacrer un droit général et absolu à l'oubli numérique sur Internet, force est de reconnaître que les réseaux sociaux, comme *Facebook*, touchent majoritairement les plus jeunes, qui sont le plus souvent les plus fragiles et les moins conscients des risques qu'une telle exposition sur ces plateformes d'échanges comporte pour leur vie privée. De surcroît, les réseaux sociaux focalisent aujourd'hui l'essentiel du temps passé sur Internet.

Or, la demande sociale de protection de la vie privée sur Internet est, dans le même temps, très forte et ne saurait, à ce titre, être ignorée. Selon l'étude réalisée en 2010 par le CRÉDOC, 91 % de la population estiment que les sites Internet devraient permettre à chacun d'effacer simplement les informations personnelles qui ont été communiquées à un moment donné et 94 % considèrent que les pouvoirs publics doivent inciter davantage les sites Internet à mieux protéger la vie privée de chacun.

C'est pourquoi, la mission a estimé qu'au regard des difficultés inhérentes et spécifiques aux réseaux sociaux (cf. *supra*) et de la demande sociale accrue en matière de protection de la vie privée, il était nécessaire d'agir et de prévoir à cette fin, pour les seuls réseaux sociaux et non l'ensemble des sites Web, un droit à l'oubli dédié et adapté, reposant sur un droit à l'effacement de ses données ainsi que la garantie d'une procédure simple et facilement accessible, permettant d'effacer l'intégralité de ses données ou de les récupérer en vue de les réutiliser.

(1) Audition du 8 septembre 2010.

Le cas des comptes inutilisés pendant une certaine durée doit également être envisagé. Une solution pourrait être de prévoir dans les clauses contractuelles liant le site à l'internaute, lorsque le compte n'est pas utilisé pendant plusieurs années, que ce dernier sera fermé et les données personnelles complètement effacées.

L'internaute disposera cependant de la faculté d'opter pour le maintien de ce compte même s'il ne fait pas l'objet d'une utilisation pendant une longue période. Ce droit d'option devra être clairement formulé au moment de l'ouverture du compte.

Orientation n° 21 : instaurer un droit à l'oubli sur les réseaux sociaux

Prévoir, pour les seuls réseaux sociaux et non l'ensemble des sites Web, un droit à l'oubli dédié et adapté, reposant sur :

— un droit exprès et effectif à l'effacement de ses données et non un simple droit à la désactivation de son profil ;

— la garantie d'une procédure simple et facilement accessible, permettant d'effacer l'intégralité de ses données ou de les récupérer en vue de les réutiliser ;

— l'effacement par principe des données d'un profil d'utilisateur après un certain délai si aucun usage n'en est fait, l'utilisateur pouvant opter pour le non-effacement de ses données.

4. Le consentement de l'utilisateur en débat : le dernier rempart contre les pratiques intrusives ?

Si la conservation de données personnelles pose la question d'un éventuel droit à l'oubli, leur collecte pose d'emblée la question du consentement de l'internaute. En effet, comme l'a indiqué à la mission, Mme Isabelle Falque-Pierrotin, présidente de l'ancien Forum des droits sur Internet [(1)], cette collecte de données personnelles est au fondement du mode de fonctionnement économique d'Internet, « son pétrole ».

Face à cette situation, la mission s'est interrogée sur la place qu'il revenait d'accorder au consentement des internautes, face aux *cookies* qui sont installés sur les ordinateurs et qui rendent possible la publicité comportementale.

(1) Audition du 2 juin 2010.

QUE SONT LES « *COOKIES* » ?

Les « *cookies* » sont de petits fichiers d'une centaine d'octets que le navigateur utilisé par l'internaute (*Internet Explorer*, *Opéra*, etc.) installe sur le disque dur de ce dernier à la demande du site consulté.

Créés en 1994 par des ingénieurs de *Netscape*, les « *cookies* » sont également appelés « mouchards électroniques » ou « témoins de connexion ». Leur objet est de permettre au site qui les a envoyés de « reconnaître » l'internaute en stockant un certain nombre d'informations : adresse IP, système d'exploitation et navigateur utilisés, pages consultées, nombre de visites du site, *etc*. En cela, les *cookies* permettent de faciliter la navigation, en mémorisant un certain nombre d'informations que l'internaute n'aura pas à ressaisir ultérieurement (par exemple, un cookie permettra à un internaute faisant ses achats en ligne de conserver en mémoire les produits placés dans le panier virtuel et de les présenter sur la facture finale).

Toutefois, les *cookies* permettent également au fournisseur de contenu ou à la régie publicitaire de conserver en mémoire un grand nombre d'informations relatives aux habitudes de navigation de l'internaute, et ce même si ce dernier possède une adresse IP dynamique et variable (cf. supra), leur offrant ainsi la possibilité de lui proposer des publicités conformes à ses préférences (telles qu'elles auront été déduites des informations collectées).

Source : Rapport d'information n° 441, op. cit.*, p. 60.*

La première solution consisterait à interdire complètement l'installation sur les ordinateurs de *cookies*. Or, les interdire assécherait une grande partie des ressources qui alimentent aujourd'hui la dynamique de l'économie numérique.

La deuxième solution reposerait sur la régulation des *cookies* par le biais du système actuel de l'*opt out* – pouvoir d'opposition, le silence de l'utilisateur valant acceptation. Cette solution ne semble cependant pas satisfaisante, car l'exercice de ce droit est d'une effectivité réduite pour l'utilisateur qui souvent ignore si des *cookies* ont été introduits ou non dans son ordinateur ou qui ne sait tout simplement pas comment les supprimer.

La troisième solution consisterait à passer au régime de l'*opt in* - consentement exprès, le silence de l'utilisateur valant refus, comme l'envisageaient M. Yves Détraigne et Mme Anne Marie Escoffier dans la proposition de loi [(1)] qu'ils ont déposée sur le bureau du Sénat le 9 novembre 2009. En effet, cette proposition de loi imposait, dans sa rédaction initiale, le consentement de l'utilisateur avant tout stockage de *cookies* sur son ordinateur.

Or, comme l'a noté le rapporteur pour la commission des Lois du Sénat, M. Christian Cointat, « *appliqué de manière trop rigide, le principe de* l'opt in *obligerait en effet les internautes à réitérer continuellement leur souhait d'accepter ou de refuser les* cookies *pour chaque site consulté, voire chaque page web. Ils se verraient ainsi contraints en pratique d'interrompre leur navigation pour cliquer sur des fenêtres ou «* pop-up *» sur leur écran, ce qui, d'une part, constituerait une entrave à la navigation fluide et rapide des internautes, d'autre*

(1) Proposition de loi n° 93, session ordinaire 2009-2010, visant à mieux garantir le droit à la vie privée à l'heure du numérique, présentée par M. Yves Détraigne et Mme Anne-Marie Escoffier, enregistrée à la Présidence du Sénat le 6 novembre 2009.

part, mettrait en grandes difficultés les professionnels du commerce en ligne » [(1)]. En effet, la logique de l'*opt in* obligerait l'internaute à exprimer son consentement pour chaque entrée sur un site Internet et rendrait de fait impossible la navigation sur le réseau.

Dans ces conditions, le législateur doit-il renoncer à encadrer la pratique des *cookies* et à remettre au centre de ce dispositif le consentement de l'internaute ? La mission est convaincue de l'inverse.

Les travaux réalisés par nos collègues sur la proposition de loi précitée de M. Yves Détraigne et Mme Anne-Marie Escoffier, sont à cet égard très éclairants. En effet, rejetant la logique de l'*opt in* comme de l'*opt out* pour les raisons qui viennent d'être évoquées, les sénateurs ont, à l'initiative du rapporteur, préféré permettre à l'utilisateur d'exprimer un choix préalable et éclairé en matière de *cookies*. Afin de parvenir à cet objectif, deux leviers d'action sont envisagés.

En premier lieu, l'article 6 de la proposition de loi telle qu'elle a été adoptée par le Sénat en première lecture, le 23 mars 2010, entend améliorer l'information des internautes sur les « *cookies* » comportementaux. En effet, une meilleure connaissance du fonctionnement et des finalités de ces *cookies* ne peut que rendre les individus acteurs de leur propre protection. Une information spécifique, claire, accessible, permanente garantit dans ces conditions un choix éclairé en fonction du bilan avantages/inconvénients ressenti en matière de *cookies*.

Dans cette perspective, l'article 6 de la proposition de loi prévoit que « *le responsable du traitement ou son représentant informe, dans une rubrique spécifique et permanente ainsi que de manière claire et accessible, tout utilisateur d'un réseau de communication électronique : de la finalité des actions tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement ; de la nature des informations stockées ; des personnes ou catégories de personnes habilitées à avoir accès à ces informations ; des moyens dont l'utilisateur dispose pour exprimer ou refuser son consentement* ». Cette obligation d'information réalisée de manière globale, et non au cas par cas, concerne les seuls *cookies* comportementaux qui comprennent des informations sur les habitudes de navigation de l'internaute, excluant ainsi les *cookies* techniques, dits « de session » strictement nécessaires à la navigation.

La mission ne peut que se féliciter d'une telle démarche et souscrire à cette obligation d'information incombant aux responsables collectant des données personnelles, notamment à des fins de ciblage publicitaire. Il semble néanmoins nécessaire de compléter cette information :

---

(1) Rapport n° 330, session ordinaire 2009-2010, de M. Christian Cointat au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur la proposition visant à mieux garantir le droit à la vie privée à l'heure du numérique,, op. cit.*, p. 21.*

— d'une part, par la désignation d'un point de contact clairement identifiable pour pouvoir exercer ultérieurement ses droits d'accès, de rectification et d'opposition ;

— d'autre part, par la traduction dans la langue d'origine de l'internaute des conditions d'utilisation de ses données personnelles.

Dans ces conditions, l'internaute sera en mesure de consentir librement et de manière éclairée à l'installation de *cookies* sur son ordinateur et ainsi de bénéficier ou non de publicités ciblées suivant ses besoins.

Orientation n° 22 : renforcer l'information des internautes en matière de ciblage publicitaire

Obliger les responsables de traitement collectant des données à caractère personnel par le biais de « *cookies* », notamment à des fins de ciblage publicitaire, d'informer l'internaute dans sa langue d'origine :

— des finalités et l'utilisation qui est faite de ses données de navigation ;

— de la nature des données personnelles ainsi collectées ;

— des personnes ou catégories de personnes habilitées à avoir accès à ces informations ;

— des moyens dont l'utilisateur dispose pour exprimer ou refuser son consentement ;

— des coordonnées d'un point de contact lui permettant ultérieurement d'exercer ses droits d'accès, de rectification et d'opposition.

En second lieu, afin de permettre à l'utilisateur d'exprimer un choix préalable et éclairé en matière de *cookies*, l'article 6 de la proposition de loi précitée se refuse à trancher le débat entre l'*opt in* et l'*opt in*. En effet, ils considèrent à bon droit que la directive du 18 décembre 2009 modifiant la directive « *Vie privée et communications électroniques* » du 12 juillet 2002, en ne tranchant pas la question de savoir si le silence de l'utilisateur vaut refus ou acceptation, a renvoyé la question du choix de l'utilisateur aux possibilités de paramétrage des navigateurs Internet, dont les dernières évolutions consistent notamment à offrir aux internautes de nombreuses possibilités de paramétrage en matière de « *cookies* ».

Dans cette perspective, la mission estime indispensable que les navigateurs Internet permettent sur le plan technique un paramétrage fin en matière de *cookies* et répondent, pour ce faire, à deux impératifs techniques. En premier lieu, un réglage par défaut protecteur des données personnelles doit être proposé à l'internaute au moment de l'installation ou de la mise à jour du navigateur. En second lieu, ce paramétrage par défaut doit pouvoir être facile à modifier et ne pas contraindre l'utilisateur à faire un choix global – acceptation ou

refus en bloc – en matière de *cookies*. Il doit en effet permettre à l'internaute de gérer ses préférences en fonction des caractéristiques des *cookies* qui sont généralement différentes d'un site à l'autre. Dans ces conditions, le navigateur Internet offrira à l'internaute un outil de pilotage transparent pour sa navigation lequel lui permettra de dire « *oui* », « *non* » ou « *je préfère* ».

Mais, faut-il encore que l'internaute soit pleinement informé des possibilités de paramétrage de son navigateur Internet, faute de quoi il ne saurait y avoir de consentement préalable en matière de *cookies*. C'est pourquoi, l'article 6 de la proposition de loi précitée oblige le responsable de traitement ou son représentant à informer, « *dans une rubrique spécifique et permanente ainsi que de manière claire et accessible, tout utilisateur d'un réseau de communication électronique […] des moyens dont l'utilisateur dispose pour exprimer ou refuser son consentement* ».

La mission souscrit pleinement à cette démarche consistant à informer très clairement l'internaute des possibilités de réglage de son navigateur Internet en matière de *cookies* et à les expliciter, afin qu'il puisse exprimer un choix préalable éclairé. Cependant, il est impératif que, dans le même temps, les navigateurs Internet offrent aux utilisateurs un outil de pilotage fin et transparent de leurs choix.

Orientation n° 23 : développer des navigateurs Internet plus protecteurs et plus transparents en matière de ciblage publicitaire

Obliger les responsables de traitement collectant des données à caractère personnel par le biais de « *cookies* », notamment à des fins de ciblage publicitaire, d'informer l'internaute des possibilités de paramétrage dont l'utilisateur dispose depuis son navigateur Internet pour exprimer ou refuser son consentement. Il est cependant impératif que, dans le même temps, les navigateurs Internet offrent un réglage par défaut :

— protecteur des données personnelles au moment de l'installation ou de la mise à jour du navigateur ;

— transparent et facile à modifier ;

— fin, lui permettant de gérer ses préférences en fonction des caractéristiques des *cookies* et, à ce titre, de dire « *oui* », « *non* » ou « *je préfère* ».

B. PARVENIR RAPIDEMENT À UNE APPROCHE COMMUNE FORTE EN EUROPE

Après la France, l'Europe… Comme toute politique publique, la protection de la vie privée ne peut se concevoir au seul niveau national. La révision prochaine de la directive du 24 octobre 1995 relative à la protection des données personnelles offre, à cet égard, l'occasion unique de définir un niveau de protection élevé en Europe qui, si elle entend préserver notre conception de la vie privée, doit dès aujourd'hui investir massivement dans les technologies « *privacy by design* » respectueuses de la vie privée dès leur conception.

1. Un cadre juridique communautaire riche et exigeant

En matière de protection de la vie privée et des données personnelles, le droit communautaire offre un cadre juridique riche et exigeant qui repose principalement sur quatre séries de textes.

Il s'agit, en premier lieu, de la Charte européenne des droits fondamentaux du 7 décembre 2000, qui est juridiquement contraignante pour les États membres depuis l'entrée en vigueur du Traité de Lisbonne, reconnaît, à son article 7, le droit au respect de la vie privée et familiale [(1)] et, à son article 8, le droit à la protection des données à caractère personnel [(2)].

À cette charte, vient s'ajouter, en second lieu, la directive 95/46/CE du 24 octobre 1995 [(3)] 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. Cette directive, qui reprend l'essentiel des dispositions de la loi *Informatique et libertés* du 6 janvier 1978 constitue le texte européen de référence en matière de protection des données à caractère personnel. Elle assure un champ de protection large, recouvrant de multiples droits et libertés, s'inspirant en cela de l'intention exprimée par le législateur français vingt ans auparavant. La directive du 24 octobre 1995 s'applique à toutes les bases de données personnelles, tant dans le secteur public que dans le secteur privé, mais non aux traitements mis en œuvre pour l'exercice d'activités relevant, jusqu'à l'entrée en vigueur du Traité de Lisbonne, du premier pilier [(4)], telles que les activités dans les domaines de la coopération policière et judiciaire en matière pénale.

La protection des données personnelles relatives à la coopération policière et judiciaire en matière pénale est régie par la décision-cadre relative à la protection des données personnelles du 27 novembre 2008 [(5)]. Le cadre juridique ainsi établi reste cependant minimaliste dans la mesure où cette décision-cadre ne porte que sur les données à caractère personnel qui « *sont ou ont été transmises ou*

---

(1) « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications *».*

(2) « Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante *».*

(3) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(4) Le pilier communautaire correspond aux trois communautés : la Communauté européenne, la Communauté européenne de l'énergie atomique (EURATOM) et l'ancienne Communauté européenne du charbon et de l'acier (CECA) (premier pilier). Le second pilier est consacré à la politique étrangère et de sécurité commune, couverte par le titre V du traité sur l'Union européenne, alors que le troisième pilier est consacré à la coopération policière et judiciaire en matière pénale, qui est couverte par le titre VI du traité sur l'Union européenne.

(5) Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350 du 30.12.2008, p. 60).

mises à disposition entre les États membres » [1] ou entre systèmes d'informations européens et États membres. Sont expressément d'ailleurs expressément exclus du champ de cette décision-cadre les « *intérêts essentiels en matière de sécurité nationale et des activités de renseignement spécifiques dans le domaine de la sécurité nationale* » [2]. Cette décision-cadre a toutefois constitué une avancée importante dans un domaine où le besoin de normes communes pour la protection des données devenait criant.

Or, le traité de Lisbonne a non seulement supprimé l'ancienne « structure en piliers» de l'Union européenne, mais a également introduit une nouvelle base juridique pour la protection des données à caractère personnel dans l'ensemble des politiques de l'Union. En effet, l'article 16 du traité sur le fonctionnement de l'Union européenne rappelle que « *toute personne a droit à la protection des données à caractère personnel la concernant* » et confie, pour ce faire, au Parlement européen et au Conseil « *le soin de fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données* ». Dans cette perspective, la révision de la directive du 24 octobre 1995 (cf. *infra*) sera l'occasion pour l'Union européenne de se doter d'un corpus de règles générales sur la protection des données personnelles, dont l'application serait étendue aux domaines de la coopération policière et de la coopération judiciaire en matière pénale.

À la directive du 24 octobre 1995, qui demeure le texte européen de référence en matière de protection des données personnelles, s'ajoute une troisième série de textes garantissant spécifiquement le respect de la vie privée en matière de communications électroniques. Le premier texte adopté par l'Union européenne dans ce domaine est la directive 2002/58/CE du 12 juillet 2002 dite directive « vie privée et communications électroniques » [3], qui s'applique aux traitements de données personnelles, au sens de la directive précitée du 24 octobre 1995, dans le cadre de la fourniture de services de télécommunications accessibles au public dans l'Union européenne, notamment *via* les réseaux numériques mobiles.

La directive du 12 juillet 2002 impose, à cette fin, des obligations fondamentales destinées à garantir la sécurité et la confidentialité des communications sur les réseaux électroniques de l'Union européenne, y compris Internet et les services mobiles. Dans cette perspective, la directive du 12 juillet 2002 interdit notamment, à son article 13, les courriers électroniques commerciaux non sollicités – phénomène plus connu sous le nom de « *spamming* » – qui sont

(1) Article premier.
(2) Ibid.
(3) 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.

soumis au principe du consentement préalable, dit de l'« *opt in* ». Elle définit également les règles relatives à l'installation de témoins de connexion – plus connus sous le nom de « *cookies* » – sur les ordinateurs personnels des utilisateurs et à l'exploitation des données de localisation générées par les téléphones portables.

Cependant, des disparités de transposition et d'application par les États membres de cette directive du 12 juillet 2002 sont très rapidement apparues, notamment sur la possible limitation du principe d'effacement et d'anonymisation des données prévu à son article 15 [(1)]. Les institutions européennes ont été contraintes de modifier et de compléter la directive du 12 juillet 2002 par un nouveau texte, la directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques [(2)]. L'objectif poursuivi par cette directive, comme le rappelle son article premier, est « *d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques [...] en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne* ».

La directive du 12 juillet 2002 a également été modifiée à l'occasion de l'adoption par l'Union européenne à l'automne 2009 du « *Paquet Télécoms* », lui-même composé de trois textes [(3)]. L'un d'entre eux, la directive 2009/136/CE du

---

(1) L'article 15 de la directive du 12 juillet 2002 dispose que « Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne *».*

(2) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

(3) • Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.

• Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

• Règlement 1211/2009/CE du Parlement européen et du Conseil du 25 novembre 2009 instituant l'Organe des régulateurs européens des communications électroniques (ORECE) ainsi que l'Office.

25 novembre 2009, impose aux seuls fournisseurs de services de communications électroniques (opérateurs) l'obligation de notifier à la CNIL et, dans les cas les plus graves, aux utilisateurs, les violations de données personnelles, définies en un sens large : destruction, altération, transmission, etc. Cette même directive renforce au bénéfice des utilisateurs l'information relative à l'installation sur les ordinateurs personnels de « *cookies* ». En effet, son article 5-3 prévoit que « *les États membres garantissent que le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement* ».

En quatrième et dernier lieu, le cadre juridique européen en matière de la protection de la vie privée comprend des garanties spécifiques pour les données personnelles utilisées par les instances communautaires. Ces garanties sont aujourd'hui consacrées et réunies dans le règlement 45/2001/CE du Parlement européen et du Conseil, du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et les organes de l'Union européenne et à la libre circulation des données. Afin de garantir un niveau de protection élevé, ce règlement institue une instance de surveillance indépendante chargée de contrôler l'application de ces dispositions, à savoir le contrôleur européen de la protection des données, que la mission a rencontré lors de son déplacement à Bruxelles [(1)].

2. La révision de la directive du 24 octobre 1995 : parvenir à une approche globale dans l'Union européenne

Le 4 novembre dernier, la Commission européenne a publié une communication intitulée « *Une approche globale de la protection des données à caractère personnel dans l'Union européenne* », marquant ainsi le lancement de ses travaux en vue de la révision de la directive du 24 octobre 1995 sur la protection des données personnelles.

La révision de cette directive est fondamentale, puisqu'elle doit être l'occasion d'un alignement par le haut des législations nationales régissant la protection des données personnelles. En effet, certains de nos voisins européens ne partagent pas tous cette ambition et souhaitent des règles du jeu *a minima*. La mission est convaincue que la France et l'Allemagne, dont les législations ont fortement influencé la rédaction de la directive de 1995, devront à cet égard jouer un rôle moteur.

En l'état actuel, la directive du 24 octobre 1995 n'a que partiellement rempli son objectif d'une harmonisation des législations nationales en matière de protection des données personnelles. En effet, la directive reconnaît aux États membres une marge de manœuvre dans certains domaines et elle les autorise à

(1) Déplacement du 27 octobre 2010.

maintenir ou à introduire des régimes particuliers pour des situations spécifiques [1]. Ces éléments, combinés au fait que les États membres appliquent parfois incorrectement la directive, sont à l'origine de divergences entre les législations nationales la transposant.

Ce manque d'harmonisation des législations nationales s'apprécie au regard des procédures en manquement actuellement en instance devant la Cour de justice de l'Union européenne pour des infractions à la directive 95/46/CE du 24 octobre 1995. Ainsi, au 27 octobre 2010, date du déplacement de la mission à Bruxelles :

— la Commission européenne avait saisi la Cour de justice en alléguant une mauvaise application de la directive par l'Allemagne, notamment au regard de l'exigence d'indépendance des autorités nationales de contrôle. La Cour a fait droit à la demande de la Commission par un arrêt prononcé le 9 mars 2010 (affaire C-518/07) ;

— la Commission avait également décidé, quelques jours auparavant, de saisir la Cour de justice pour non-respect de la législation britannique des règles de confidentialité des communications ne respecte pas la directive. La Commission a présenté une requête à cet effet ;

— la Commission a notifié trois avis motivés (étape de procédure précédant la saisine de la Cour) à l'Allemagne, à l'Autriche et au Royaume-Uni pour leur contester différentes violations de cette directive. Elle examinait les réponses des autorités allemandes et autrichiennes et était en attente de la réponse des autorités britanniques (pour laquelle le délai n'avait pas encore expiré) avant de prendre les décisions qui s'imposent ;

— d'autres procédures étaient en phase préliminaire et n'ont pu, par conséquent, être communiquées à ce stade à la mission, pour tenir compte du devoir de confidentialité dans les relations avec les États membres dans le cadre des procédures en manquement.

Parce que cette insuffisante harmonisation est un problème majeur qui affaiblit dans son ensemble le niveau de protection des données personnelles en Europe, la mission propose qu'une étape décisive soit désormais franchie. En effet, afin de parvenir à une approche commune entre les vingt-sept États membres en matière de protection des données personnelles, elle s'interroge sur l'opportunité, dans le respect du principe de subsidiarité [2], d'adopter une nouvelle législation communautaire en la matière par voie de règlement et non de directive. Il s'agirait là d'un signal fort envoyé, d'une part, aux acteurs de

---

(1) CJCE, 2003, Bodil Lindqvist*, point 97. Voir également le considérant 9 de la directive 95/46/CE du 24 octobre 1995.*

(2) Article 5 du Traité sur l'Union européenne : « En vertu du principe de subsidiarité, dans les domaines qui ne relèvent pas de sa compétence exclusive, l'Union intervient seulement si, et dans la mesure où, les objectifs de l'action envisagée ne peuvent pas être atteints de manière suffisante par les États membres, tant au niveau central qu'au niveau régional et local, mais peuvent l'être mieux, en raison des dimensions ou des effets de l'action envisagée, au niveau de l'Union *».*

l'économie numérique, montrant combien l'Union européenne est déterminée à agir pour protéger la vie privée des individus, et, d'autre part, aux citoyens européens, leur rappelant qu'ils bénéficient d'un niveau de protection élevé et équivalent quel que soit leur pays.

Au-delà de la seule question de l'instrument juridique susceptible de porter cette nouvelle législation communautaire, la mission est convaincue que l'objectif premier de cette révision de la directive du 24 octobre 1995 est de garantir un niveau de protection élevé et homogène dans l'ensemble de l'Union européenne. L'enjeu est de taille à l'heure où la conception américaine de la vie privée, fondée sur le point de vue du consommateur, tend à s'imposer et à prendre le pas sur la conception européenne, fondée, pour sa part, sur le point de vue du citoyen.

En effet, lors de son déplacement à Washington [(1)], la mission a pu constater qu'il n'existe pas, aux États Unis, de règles générales et globales sur la protection des données personnelles sur Internet. Des réglementations protectrices existent cependant dans des secteurs spécifiques et jugés sensibles, comme les données financières [(2)], les données médicales [(3)] ou la protection de l'enfance [(4)]. Par ailleurs, les États-Unis ne disposent pas d'une autorité indépendante dédiée à la protection des données. À défaut d'avoir une telle autorité, la protection des données est assurée par la *Federal Trade Commission* et le *Department of Commerce* sous un angle strictement commercial : il s'agit de protéger le consommateur de pratiques commerciales abusives et non un droit fondamental de l'individu. Selon M. Darrel West, vice-président du centre pour l'innovation technologique au *Brookings Technology Innovation*, « *the debate over privacy is a debate over money* ».

Toutefois, avec la multiplication des atteintes à la vie privée en ligne, les dernières années ont vu émerger aux États-Unis un débat sur l'opportunité d'une régulation plus poussée en matière de protection de la vie privée en ligne. À l'heure où les Américains sont sur le point de se doter de nouvelles règles en la matière, il est essentiel que l'Europe puisse s'ériger en modèle, en garantissant dans l'ensemble de l'Union européenne un niveau de protection élevé des données personnelles. La révision de la directive du 24 octobre 1995 lui en offre l'unique occasion.

---

(1) Déplacement à Washington du 1er au 4 février 2011.

(2) Le Fair Credit Reporting Act*, voté en 1970, encadre les fichiers relatifs à la situation financière des individus pour l'accès au crédit.*

(3) Le Health Insurance Portability and Accountability Act*, voté en 1996, encadre la collecte, l'enregistrement, l'usage et la diffusion des données médicales.*

(4) Le Children's Online Privacy Protection Act*, voté en 1998, interdit aux sites Internet de collecter des informations sur les mineurs de moins de 13 ans.*

Orientation n° 24 : assurer et préserver un haut niveau de protection des données en Europe

Dans le cadre de la révision de la directive du 24 octobre 1995, garantir un niveau de protection élevé et équivalent des données personnelles dans l'ensemble de l'Union européenne, en instaurant une nouvelle législation communautaire, le cas échéant, par voie de règlement.

Mise à part la question de l'instrument juridique de cette révision de la directive du 24 octobre 1995, la mission estime que l'élaboration de la nouvelle législation communautaire en matière de protection des données personnelles devra répondre à trois enjeux : la notification des failles de sécurité, les obligations incombant aux responsables de traitement et le *cloud computing*.

S'agissant en premier lieu des failles de sécurité, les administrations, les opérateurs et les entreprises qui procèdent au traitement de données à caractère personnel s'efforcent d'en assurer la sécurité en mettant en place des systèmes qui ne sont pas toujours sans failles, comme l'ont récemment illustré en France l'incident dont a été victime la SNCF en mars 2010 et en Allemagne les fuites de données provoquées par *Google Street View*.

En France, le responsable du traitement des données à caractère personnel est aujourd'hui tenu d'une obligation de moyens en vertu de laquelle il doit prendre « *toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* » (1).

La question se pose de savoir si cette obligation de moyens doit devenir une obligation de résultat et s'il faut instaurer une obligation de double notification des violations de traitement de données à caractère personnel. Ainsi le responsable du traitement serait tenu de les notifier sans délai à la Commission nationale de l'informatique et des libertés (CNIL) et si les violations venaient à affecter les données à caractère personnel d'une ou plusieurs personnes physiques, il serait tenu d'en informer ces personnes.

Dans sa communication précitée du 4 novembre 2010 et intitulée «*Une approche globale de la protection des données à caractère personnel dans l'Union européenne* », la Commission s'est engagée à « *examiner les modalités d'introduction, dans le cadre juridique global, d'une obligation générale de notification des violations de données à caractère personnel, indiquant les destinataires de ce type de notifications et les critères auxquels serait subordonnée l'application de cette obligation* ».

En effet, l'article 7 de la directive « Vie privée » du paquet Télécoms du 25 novembre 2009, comme les mesures de transposition qu'il est prévu d'adopter

(1) Article 34 de la loi du 6 janvier 1978.

en France par ordonnance [(1)], impose d'ores et déjà aux seuls fournisseurs de services de communications électroniques une obligation de notification des failles de sécurité auprès de l'autorité nationale compétente et des particuliers concernés. Or, le considérant 59 de la directive précitée souligne que « *l'intérêt des utilisateurs à être informés ne se limite pas, à l'évidence, au secteur des communications électroniques* » et qu'« *il convient dès lors d'introduire de façon prioritaire, au niveau communautaire, des exigences de notification explicites et obligatoires, applicables à tous les secteurs* ».

C'est pourquoi, la mission souhaite que, dans le cadre de la révision de la directive du 24 octobre 1995, soit consacrée l'obligation pour tout responsable de traitements de données à caractère personnel de notifier les failles de sécurité auprès de l'autorité nationale de protection des données personnelles – en France, la CNIL – et des particuliers concernés par ces violations.

Orientation n° 25 : obliger tout responsable de traitements à notifier les failles de sécurité

Dans le cadre de la révision de la directive du 24 octobre 1995, consacrer l'obligation pour tout responsable de traitements de données à caractère personnel de notifier les failles de sécurité auprès de l'autorité nationale de protection des données personnelles – en France, la CNIL – et des particuliers concernés par ces violations.

S'agissant en deuxième lieu des obligations qui doivent incomber à tout responsable d'un traitement de données à caractère personnel, la révision de la directive du 24 octobre 1995 doit être l'occasion d'étendre de manière significative ces obligations afin de renforcer l'information des individus dont les données personnelles sont collectées.

La Commission européenne semble partager cette préoccupation, puisque, dans sa communication précitée du 4 novembre 2010, elle s'est engagée à « *responsabiliser davantage les responsables de traitement* » et à définir, à cette fin, plus clairement leurs obligations, notamment en matière d'information des personnes dont les données personnelles sont collectées.

En l'état actuel, les articles 10 et 11 de la directive du 24 octobre 1995 disposent que « *le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations énumérées ci-dessous : l'identité du responsable du traitement et, le cas échéant, de son représentant ; les finalités du traitement auquel les données sont destinées ; toute information supplémentaire telle que les destinataires ou les catégories de destinataires des données ; le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse ; l'existence d'un droit d'accès aux données la concernant et de rectification de ces données* ».

(1) Art. 17 de la loi n° 2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de communications électroniques.

L'article 32 de la loi n° 78-17 du 6 janvier 1978 qui transpose ces dispositions va légèrement au-delà des exigences communautaires, puisqu'il prévoit, pour sa part, que la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est également informée, le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non-membre de l'Union européenne.

Les évolutions technologiques récentes et les nouvelles plateformes d'échanges, en démultipliant le nombre de données personnelles collectées chaque jour, exigent que les personnes concernées bénéficient au préalable d'une information renforcée et ce, n'importe où en Europe. C'est pourquoi, la mission propose que, dans le cadre de la révision de la directive du 24 octobre 1995, les informations que le responsable de traitement est tenu de donner aux personnes concernées soient étendues aux coordonnées du responsable du traitement et, le cas échéant, de celle de son représentant, à la durée de conservation des données collectées et aux critères qui la justifient ainsi qu'aux coordonnées du service auprès duquel les droits d'accès, de rectification et de suppression peuvent s'exercer.

Il est indispensable que cette information préalable soit délivrée à l'utilisateur de manière spécifique, claire et accessible, ce qui implique notamment qu'elle fasse l'objet d'une traduction dans sa langue d'origine, laquelle devra, plus largement, concerner les conditions d'utilisation ainsi que les rubriques « *privacy* ».

Orientation n° 26 : renforcer l'information des personnes dont les données personnelles sont collectées

Dans le cadre de la révision de la directive du 24 octobre 1995, renforcer les obligations d'information incombant à tout responsable collectant des données personnelles, qui devront désormais informer de manière spécifique, claire et accessible la personne concernée :

— des coordonnées du responsable du traitement et, le cas échéant, de celle de son représentant ;

— de la durée de conservation des données collectées et des critères qui la justifient ;

— des coordonnées du service auprès duquel les droits d'accès, de rectification et de suppression peuvent s'exercer.

Ces informations et, plus largement, les conditions d'utilisation ainsi que les rubriques « *Vie privée* » devront impérativement être traduites dans la langue d'origine de l'utilisateur.

S'agissant enfin du *cloud computing* ou, en français, « l'informatique dans les nuages », la mission a été frappée lors de ses travaux par le nombre croissant de données informatiques gérées par les particuliers, les entreprises, voire les

administrations, qui ne sont plus enregistrées sur des serveurs leur appartenant mais, au contraire, qui sont hébergées sur des supports localisés dans des pays relevant de législations très hétérogènes. Ces serveurs étant mis en réseau, il s'avère désormais de plus en plus difficile de dire où est stockée, à un instant précis, telle ou telle donnée.

Il est indéniable que le *cloud computing* offre à de nombreuses entreprises des perspectives d'économies de gestion importantes en leur permettant d'externaliser une partie de leurs services informatiques. Il constitue d'ailleurs un marché financier en pleine croissance, des grandes sociétés telles que *Google* et Microsoft proposant d'ores et déjà des plateformes d'externalisation de services.

Mais cette exportation de données sur le réseau pose des problèmes juridiques complexes car les informations traitées peuvent contenir des données personnelles, voire sensibles. Dans sa communication précitée du 4 novembre 2010, la Commission européenne a ainsi souligné que le *cloud computing* était un défi en matière de protection des données personnelles, car il « *peut signifier, pour le particulier, une perte de contrôle sur les informations potentiellement sensibles le concernant, lorsqu'il stocke ses données à l'aide de programmes hébergés sur l'ordinateur de quelqu'un d'autre* ». Par ailleurs le *cloud computing* conduit à multiplier la création de *data centers*, dont il est impossible d'affirmer *a priori* si la sécurité y est assurée.

C'est pourquoi, s'interrogeant sur les garanties de confidentialité et de sécurité que présentent ces bases, la mission estime que la révision de la directive du 24 octobre 1995 doit être l'occasion de poser, de manière inédite, les bases d'une réglementation européenne en matière de *cloud computing*. Celle-ci pourrait emprunter deux voies complémentaires.

Afin d'assurer la confidentialité des données, il conviendrait d'exclure du *cloud computing* réalisé hors de l'Union européenne le traitement de données personnelles sensibles ou comportant certains risques pour les personnes concernées (c'est-à-dire données biométriques, données génétiques, données judiciaires, données financières, données concernant des enfants).

Orientation n° 27 : exclure du *cloud computing* réalisé hors Union européenne les données personnelles dites « sensibles »

Dans le cadre de la révision de la directive du 24 octobre 1995, exclure du *cloud computing* réalisé hors de l'Union européenne le traitement de données personnelles sensibles ou comportant certains risques pour les personnes concernées, comme les données biométriques, les données génétiques, les données judiciaires, les données financières ou les données concernant des enfants.

S'agissant ensuite de la sécurité des bases de données, celle-ci pourrait être garantie par l'obligation faite aux acteurs du *cloud computing* de réaliser régulièrement des audits de sécurité.

Orientation n° 28 : soumettre les acteurs du *cloud computing* à des audits de sécurité réguliers

Dans le cadre de la révision de la directive du 24 octobre 1995, faire obligation aux acteurs du *cloud computing* de réaliser régulièrement des audits de sécurité.

Cependant, le succès de la révision de la directive du 24 octobre 1995 dans ces trois domaines – notification des failles de sécurité, obligations incombant aux responsables de traitement et *cloud computing* – requiert que le mode de fonctionnement du G29 soit révisé et clarifié.

Le G29 est un organe consultatif européen indépendant sur la protection des données et de la vie privée, créé en application de l'article 29 de la directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (1).

Ce groupe de travail européen réunit à Bruxelles en séance plénière, tous les deux mois environ, les représentants de vingt-sept autorités indépendantes de protection des données nationales. Ses principales missions sont de rendre des avis sur le niveau de protection dans les pays extra-communautaires, de conseiller la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles et d'adopter des recommandations générales dans ce domaine.

Cependant, si la qualité des travaux et des avis du G29 est unanimement reconnue, il se caractérise, comme l'a indiqué le président de la CNIL à la mission (2), par un manque d'indépendance qui le fragilise. En effet, le G29 ne dispose pas de moyens propres : son secrétariat est assuré par l'unité chargée de la protection des données à la direction générale « Justice, Liberté et Sécurité » de la Commission européenne. La présidence du G29 génère également de nombreux coûts pour le pays d'origine du président de cet organe, ce qui réserve ce poste aux

(1) Article 29 « Groupe de protection des personnes à l'égard du traitement des données à caractère personnel *» de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données :*

« 1. Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé « groupe ». Le groupe a un caractère consultatif et indépendant.

« 2. Le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission. Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci procèdent à la nomination d'un représentant commun. Il en va de même pour les autorités créées pour les institutions et organismes communautaires.

« 3. Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle.

« 4. Le groupe élit son président. La durée du mandat du président est de deux ans. Le mandat est renouvelable.

« 5. Le secrétariat du groupe est assuré par la Commission.

« 6. Le groupe établit son règlement intérieur.

« 7. Le groupe examine les questions mises à l'ordre du jour par son président, soit à l'initiative de celui-ci, soit à la demande d'un représentant des autorités de contrôle ou de la Commission *».*

(2) Audition du 19 mai 2010.

représentants des plus grands États européens. Enfin, outre le fait que cette autorité ne bénéficie pas des moyens nécessaires à l'exercice de ses missions, il existe au sein des institutions européennes des situations aberrantes telles que la nomination de quatre Américains parmi un groupe de travail de cinq experts chargés examiner le contenu de la future directive européenne sur la protection des données personnelles.

C'est pourquoi, la mission estime qu'il est nécessaire que l'indépendance du groupe de travail G29 soit clairement établie et qu'il soit, à cette fin, doté de moyens humains et financiers propres. C'est à ce prix seulement qu'il pourra garantir une application uniforme des règles de protection des données de l'Union européenne au niveau national et ainsi assurer un niveau de protection équivalent.

Orientation n° 29 : renforcer l'indépendance du groupe de travail G29

Dans le cadre de la révision de la directive du 24 octobre 1995, renforcer l'indépendance du groupe de travail G29, en le dotant de moyens humains et financiers propres.

3. La technologie au service de la vie privée : faire du « *privacy by design* » un facteur de compétitivité en Europe

En février 2010, le président et fondateur de *Facebook*, M. Marc Zuckerberg, a affirmé que le souci de préserver sa vie privée « *n'était plus la norme* ». En août de la même année, le président-directeur général de *Google*, M. Éric Schmidt, n'a pas hésité à affirmer que l'anonymat sur Internet était voué à disparaître et qu'il serait remplacé par une « *transparence totale* ». La mission s'oppose fermement à la position de ces deux acteurs d'Internet, pour qui le concept de vie privée aurait changé et devrait être adapté à l'évolution des technologies numériques. Il faut, au contraire, préserver nos libertés individuelles et conserver notre conception de la vie privée, en adaptant pour ce faire pour les nouvelles technologies. Il convient dans cette perspective de se demander comment la technologie peut venir au secours de la technologie.

Le concept de *privacy by design*, que l'on traduit par « prise en compte de la vie privée dès la conception » des nouvelles technologies, offre à cet égard des perspectives encourageantes.

Ainsi, M. Marc Mossé, directeur des affaires publiques de la société Microsoft France [(1)], a indiqué à la mission que le navigateur de Microsoft *Internet Explorer 9* était conçu de telle sorte que l'internaute puisse choisir de naviguer avec ou sans *cookies*. Il s'agit là d'une option essentielle car, comme cela a été précédemment indiqué, les navigateurs Internet sont les portes d'entrée sur le Web. De même, chaque utilisateur de *MSN Messenger*, au moment où il s'inscrit à ce service, a la possibilité de fixer lui-même le champ de ses connexions de partage et donc de dimensionner sa protection en trouvant un point d'équilibre

(1) Audition du 14 septembre 2010.

entre « *le plaisir et l'oubli* ». La société Microsoft développe enfin une technologie dite « *U-Prove* » qui permet de crypter ses échanges et de choisir le degré de partage de ses informations.

De la même manière, M^e^ Winston Maxwell (1) a rappelé les perspectives offertes par la prise en compte de la vie privée dès la conception des outils informatiques. Ainsi, les projets relatifs aux réseaux d'électricité intelligents - *smart electric grid* – qui sont conçus pour calculer la fourniture d'électricité en fonction des faits et gestes du consommateur à son domicile soulignent qu'il est nécessité de trouver un équilibre entre le respect de la vie privée car de tels procédés peuvent permettre de connaître les habitudes et le rythme de vie des usagers et les impératifs d'intérêt public – dans le cas d'espèce les économies d'énergie et la lutte contre le réchauffement de la planète. Le développement du *privacy by design* peut à cet égard apporter des solutions

Les promesses, dont semble porteur le développement des technologies respectueuses de la vie privée dès leur conception, font l'objet d'une attention particulière de la part des pouvoirs publics et des autorités de contrôle. En effet, une recommandation du Parlement européen à l'attention du Conseil en date du 26 mars 2009 (2) encourage « *la promotion du principe* « privacy by design » *selon lequel la protection des données et de la vie privée devrait être introduite dès que possible dans le cycle de vie des nouveaux développements technologiques, assurant aux citoyens un environnement convivial* » et respectueux de leur vie privée.

La révision de la directive précitée du 24 octobre 1995 n'échappera d'ailleurs pas à cette question, comme semble l'indiquer la Commission européenne dans sa communication précitée du 4 novembre 2010, dans laquelle elle envisage de « *poursuivre la promotion […] des possibilités d'application concrète de la notion de prise en compte du respect de la vie privée dès la conception* », le principe de *privacy by design* étant appelé à jouer un rôle important pour garantir tant la confidentialité que la sécurité des données.

De la même manière, le groupe de travail G29, qui réunit les autorités de protection des autorités européennes, recommande que les nouvelles technologies soient conçues avec un paramétrage par défaut favorable au respect de la vie privée et ce, de manière contraignante. Comme le rappelle M. Alex Türk, « *dans son esprit, cela signifie que la collecte des données devrait être limitée, que les personnes concernées devraient bénéficier d'un bon niveau d'information et disposer de pouvoirs de contrôle plus importants, que les données devraient bénéficier d'un haut niveau de sécurité* » (3).

(1) Audition du 10 novembre 2010.

(2) Recommandation du Parlement européen du 26 mars 2009 à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur Internet (2008/2160).

(3) Alex Türk, op. cit.*, p. 152-153.*

La dernière conférence internationale « Informatique et libertés », qui s'est tenue à Jérusalem en octobre 2010 et qui a réuni l'ensemble des autorités nationales de protection des données, a d'ailleurs été l'occasion de souligner l'importance de ce nouveau principe, puisqu'une résolution sur la prise en compte de la vie privée dès la conception a été adoptée. Partant de l'insuffisance en l'état actuel aussi bien des réglementations que des initiatives politiques en matière de respect de la vie privée et de protection des données personnelles, elle dispose que « *seule l'inclusion de la vie privée dans la conception des systèmes et des traitements pourra y parvenir* ».

Ce concept se présente donc comme très prometteur pour réduire le décalage entre une technologie qui connaît un rythme de développement très rapide et les moyens de protection de la vie privée des individus, dont le niveau a toujours un temps de retard. C'est pourquoi, la mission considère qu'il revient dès aujourd'hui aux législateurs national et européen de permettre aux différents acteurs concernés de collaborer entre eux afin de rendre applicables ces nouvelles normes de sécurité et ainsi de rendre effective, en Europe, une véritable politique industrielle du numérique fondée sur le *privacy by design*.

En effet, pour élaborer de telles normes, il faut que les différentes autorités administratives, nationales et européennes, en charge de la protection des données personnelles, des réseaux et des communications électroniques, travaillent de concert avec les acteurs de l'industrie numérique. Aucun État, aucun organisme ne pourra, seul, rendre effective la notion de *privacy by design*. Or une fois que l'outil est conçu et produit par une compagnie industrielle, il est trop tard pour imposer des exigences techniques de protection. Les acteurs publics en sont alors réduits à prévenir en aval les pertes accidentelles de données.

Grâce au renforcement de la recherche et du développement que la mission appelle de ses vœux dans le secteur des technologies respectueuses de la vie privée dès leur conception, dites « *privacy by design* », l'Union européenne sera enfin en mesure de se doter d'une véritable politique industrielle du numérique et ainsi de bénéficier d'un indéniable avantage comparatif dans la compétition mondiale, lui permettant d'attirer de nouveaux acteurs et de gagner des parts de marché.

Orientation n° 30 : faire du « *privacy by design* » un atout majeur pour l'Europe

Encourager et renforcer au sein de l'Union européenne la recherche, l'innovation et le développement dans le secteur des technologies respectueuses de la vie privée dès leur conception, dites « *privacy by design* », afin de doter l'Europe d'une véritable politique industrielle du numérique et lui permettre ainsi de bénéficier d'un indéniable avantage comparatif dans la compétition mondiale.

C. INVENTER AU NIVEAU INTERNATIONAL UNE PROTECTION INÉDITE ET EFFICACE DE LA VIE PRIVÉE

Si la révision de la directive du 24 octobre 1995 doit permettre l'édification d'une approche commune au sein de l'Union européenne, il ne s'agit là que d'une première étape vers la définition d'un instrument international de protection des données.

En effet, le propre d'Internet est d'être un réseau mondial où les acteurs - éditeurs, hébergeurs, fournisseurs d'accès – peuvent être situés dans n'importe quel pays. Il convient donc dès aujourd'hui de renforcer activement la coopération internationale sur les questions de respect de la vie privée afin de parvenir à une protection équivalente depuis n'importe quel point du globe.

1. Un cadre juridique international parcellaire et peu contraignant

Si la protection de la vie privée et des données à caractère personnel a fait l'objet d'une reconnaissance internationale depuis la fin de la Seconde guerre mondiale, elle n'obéit aujourd'hui à aucun cadre juridique universel et contraignant. En effet, seules des initiatives isolées, dans le cadre du Conseil de l'Europe, de l'Organisation de la coopération et du développement économique (OCDE) ou des Nations unies, ont été prises à jour. Certaines de ces initiatives ont permis l'adoption d'instruments juridiques internationaux, dont l'application et le respect dépendent de la bonne volonté des États. D'autres, en revanche, se contentent de suggérer aux autorités nationales de bonnes pratiques, quand elles ne sont pas la simple mise en forme d'intentions affichées par les États en matière de respect de la vie.

Au nombre de ces initiatives qui ont été prises sur la scène internationale, il convient en premier lieu de citer l'action de l'Organisation des Nations unies (ONU), qui s'appuie sur l'article 12 de la Déclaration universelle des droits de l'homme du 10 décembre 1948, aux termes duquel « *nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* » [(1)].

Dans cette perspective, les Nations unies ont engagé une réflexion sur la protection de la vie privée et des données à caractère personnel. Cette réflexion a conduit à l'élaboration et à l'adoption par l'assemblée générale en 1990 [(2)] de lignes directrices, aux termes desquelles le droit des personnes ainsi que l'autorité de contrôle dont la mise en place est conseillée sont au cœur du dispositif de protection de la vie privée et des données personnelles. Ces lignes directrices, qui n'ont pas de valeur juridique contraignante, définissent un certain nombre de

(1) Il convient de noter qu'une rédaction similaire a été reprise lors de l'élaboration de l'article 17.1 du Pacte international relatif aux droits civils et politiques du 16 novembre 1966, qui est entré en vigueur le 23 mars 1976.

(2) Nations unies, résolution n°45-95, 14 décembre 1990.

garanties, notamment en ce qui concerne les données sensibles, dont le périmètre est assimilé à celui des données susceptibles de donner lieu à des discriminations illicites ou arbitraires, incluant les informations sur les origines raciales ou ethniques, la couleur, la vie sexuelle, les opinions politiques, philosophiques ou autres, comme l'appartenance à une association ou à un syndicat.

La réflexion engagée par les Nations unies ne fait toutefois pas figure de pionnière. En effet, dix années auparavant, l'OCDE avait publié ses propres lignes directrices, qui figurent dans une recommandation du 23 septembre 1980 fixant « *les lignes directrices régissant la protection de la vie privée et le flux transfrontalier de données à caractère personnel* ». Cette recommandation, comme les lignes directrices des Nations unies, n'a pas de valeur obligatoire, mais incite les États à veiller au bon équilibre dans ce domaine et, dans cette perspective, à répondre à deux types d'obligations : une obligation de protection de la vie privée et des libertés individuelles et une obligation d'assurer la libre circulation des données.

Sur l'obligation de protection de la vie privée et des libertés individuelles, les États doivent veiller à la collecte et à la qualité des données ainsi que le respect des principes de finalité, de sécurité et de transparence. Les États sont tenus, en outre, d'assurer le droit d'accès et de contestation et d'organiser la responsabilité du gestionnaire du fichier.

Sur l'obligation d'assurer la libre circulation des données, les pays membres, qui sont liés par une obligation d'information et d'assistance mutuelle, doivent s'efforcer de vérifier les conséquences sur les autres pays membres, assurer la sécurité du flux transfrontalier des données et prendre toutes mesures appropriées. Ils sont notamment tenus d'adopter des lois adaptées, de favoriser et de soutenir les systèmes d'autoréglementation, de faciliter la mise en œuvre du droit des personnes physiques, de prévoir les sanctions et les recours et, enfin, de veiller à l'absence de discrimination.

À côté des actions entreprises par les Nations unies et l'OCDE, l'initiative internationale la plus aboutie et la plus formalisée à ce jour sur le plan juridique en matière de protection de la vie privée demeure incontestablement celle engagée par le Conseil de l'Europe.

L'action de ce dernier trouve son fondement de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, adoptée le 4 novembre 1950, aux termes duquel « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». Faisant

application de cette disposition, la Cour européenne des droits de l'homme a également défini une jurisprudence protectrice des intérêts des particuliers : le droit au respect de la vie privée dont ils bénéficient impose aux États d'édicter un ensemble de dispositions législatives permettant d'en assurer la protection [(1)].

Soucieux de définir un cadre juridique cohérent sur la protection de la vie privée et des données personnelles, le Conseil de l'Europe s'est progressivement doté d'un ensemble de textes, parmi lesquels figure la Convention STE 108 du 28 janvier 1981 [(2)] relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Cette convention, qui garantit spécifiquement « *à toute personne physique […] le respect […] de son droit à la vie privée à l'égard du traitement automatisé des données à caractère personnel la concernant* », a constitué, à l'échelle européenne, le premier instrument international juridiquement contraignant, ayant pour double objectif d'une part de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel et, d'autre part, de réglementer les flux transfrontaliers des données.

Elle prévoit à cette fin plusieurs garanties en matière de traitement des données à caractère personnel. D'une part, elle proscrit le traitement des données « *sensibles* » relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle et aux condamnations pénales en l'absence de garanties offertes en droit interne. Elle garantit, d'autre part, le droit des personnes concernées de connaître les informations stockées à leur sujet et d'exiger le cas échéant des rectifications, sauf lorsque les intérêts majeurs de l'État (sécurité publique, défense, etc.) sont en jeu. La convention impose enfin des restrictions aux flux transfrontaliers de données dans les États où n'existe aucune protection équivalente.

Le cadre juridique international qui s'est dessiné en matière de protection de la vie privée et des données personnelles apparaît donc relativement fragmenté et peu contraignant pour les États. En l'absence de cadre juridique universel, c'est bien l'hétérogénéité des droits nationaux qui prévaut, offrant aux individus des niveaux de garantie et de protection très variables suivant le droit applicable.

2. Le respect de la vie privée à l'épreuve de l'extraterritorialité

Or, la question de savoir quel est le droit applicable en matière de protection de la vie privée se pose aujourd'hui avec d'autant plus d'acuité que la mondialisation s'est traduite par une intensification des flux transfrontaliers de données personnelles, alors même que les systèmes juridiques nationaux se caractérisent par des différences d'approche en matière de protection des données personnelles. Ainsi, lorsque les individus veulent, à l'encontre d'un acteur d'Internet basé à l'étranger, exercer leur droit au respect de la vie privée dans le

(1) CEDH, Marckx c. Belgique*, 13 juin 1979.*
(2) Entrée en vigueur le 1er octobre 1985.

cadre de la législation nationale, ils se voient opposer par le juge le principe dit d'extraterritorialité, qui fait obstacle à l'application de la législation et aux garanties qu'elle comporte.

Ainsi, en 2008, le juge des référés du tribunal de grande instance de Paris a été saisi par une requérante qui, en application des garanties reconnues par la loi *Informatique et libertés* du 6 janvier 1978, ne voulait plus voir apparaître sur le moteur de recherche *Google*, après une requête à partir de ses nom et prénom, ses messages postés quelques années auparavant sur des groupes de discussion. Le juge a refusé d'ordonner la suppression des archives en question des serveurs de *Google Groupes* ainsi que des informations relatives à ses nom et prénom stockés dans les index ou la mémoire cache du moteur de recherche. Se fondant sur l'article 4 de la directive précitée du 24 octobre 1995, qui écarte son applicabilité aux traitements dont les responsables sont situés en dehors de l'Union européenne, même si lesdits traitements visent un public situé sur le territoire européen, il a jugé que la loi *Informatique et libertés* n'était pas applicable. Les serveurs de *Google* étant établis en Californie, il a estimé que le droit californien s'appliquait de plein droit [(1)].

En effet, en matière de protection de la vie privée et des données à caractère personnel, les grands acteurs de l'Internet, comme *Google* ou *Facebook*, dont le siège est basé aux États-Unis, ne sont pas, en raison du principe d'extraterritorialité, soumis à la loi française *Informatique et libertés*, mais bien aux lois américaines de protection des données et aux juridictions des États fédérés.

Les règles relatives au droit applicable semblent toutefois faire l'objet d'interprétations divergentes. Ainsi, le 15 mars 2011, dans une ordonnance de référé, le tribunal de grande instance de Montpellier a ordonné à *Google Inc.* de supprimer de ses moteurs de recherche tous les résultats apparaissant à la suite des requêtes avec les nom et prénom d'une femme associés aux termes « *swallows* » [(2)] et « *école de Laetitia* », qui renvoyaient tous deux directement ou indirectement vers une ancienne vidéo à caractère pornographique la mettant en scène. Le tribunal a considéré que ces résultats constituaient un trouble manifestement illicite du fait de l'inaction de *Google* à désindexer les pages web litigieuses et de l'atteinte à l'intimité de la vie privée de la plaignante.

En plus de l'atteinte à la vie privée, le tribunal s'est fondé sur la loi *Informatique et libertés* du 6 janvier 1978 pour rendre son jugement. Il a d'abord reconnu que cette législation était applicable au moteur de recherche *Google*, traitement de données dont *Google Inc.* est le responsable. En conséquence, « *il lui incombe d'aménager la possibilité d'un retrait* a posteriori *des données à caractère personnel en permettant la désindexation des pages à la demande de la personne concernée par ces données en application [du droit d'opposition prévu*

(1) Tribunal de grande instance de Paris Ordonnance de référé 14 avril 2008 - Bénédicte S contre Google Inc., Google France.

(2) En français, « hirondelles *».*

à] l'article 38, alinéa 1er de la loi précitée ». Le juge des référés a tranché la question de l'application de la loi *Informatique et libertés* à *Google Inc.*, société de droit américain dont les serveurs sont situés outre-Atlantique, en s'appuyant sur l'article 5 de cette loi qui définit les règles de compétence territoriale de ses dispositions et qui prévoit notamment qu'est soumis à la loi du 6 janvier 1978 « *le responsable de traitement qui, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français* ». La société *Google Inc.* remplissant cette condition, le juge des référés a estimé que la loi *Informatique et libertés* du 6 janvier 1978 s'appliquait à elle.

L'absence de règles européennes et internationales claires et précises sur la détermination du droit applicable a également donné lieu à la mise en place de stratégies individuelles de la part des acteurs de l'Internet, qui cherchent tantôt à se conformer aux législations nationales, tantôt à les contourner.

Ainsi, sur la question de la prise en considération du droit national français par la société *Google*, ses représentants ont indiqué à la mission que *Google* avait développé sa propre politique en la matière et ce, à défaut de règles internationales fixant les critères d'application du droit interne lorsque le service est matériellement localisé à l'étranger. Différents critères sont pris en compte, notamment l'implantation d'une filiale de la société dans le pays et l'existence d'une activité de promotion commerciale. Si ces deux critères sont remplis, la société *Google* prend en compte la législation locale. Un travail de formation au plan interne est également effectué afin de traiter les réclamations des internautes en conformité avec le droit national.

Par ailleurs, la société *Google* dispose d'une technologie capable de bloquer, sur un territoire considéré, les contenus illicites tout en les maintenant accessibles dans les pays qui les considèrent comme licites. Ce système de blocage permet pour certains services un traitement différencié des internautes en fonction de leur origine géographique et est respectueux des frontières juridiques. Deux possibilités techniques peuvent être mises en œuvre. D'une part, la version locale d'un site peut faire l'objet d'un retrait. D'autre part, une même plateforme peut faire l'objet de degrés d'accès différents selon les contenus ; par exemple, certains résultats de recherches sur *Google.fr* peuvent être supprimés sur demande des autorités judiciaires françaises, mais ces résultats demeureront référencés pour les autres internautes qui utiliseront par exemple la version *Google.com* du moteur de recherche. De la même manière, il est possible sur la plateforme *YouTube* de faire-valoir les droits d'auteurs de manière différenciée selon les pays, en autorisant le visionnage en fonction des zones géographiques des internautes.

En revanche, il ressort des échanges avec la mission que la société *Google* ne tient pas compte des législations des pays où elle n'est pas implantée. Cette position peut alors être source de tensions avec les pays concernés, dans la mesure où les services de *Google* y sont tout de même accessibles. La mission regrette qu'une telle politique puisse conduire à d'éventuelles stratégies d'évitement. En

effet, si la société *Google* souhaite se soustraire à une législation nationale, il lui suffit de fermer sa représentation dans le pays concerné.

La révision de la directive précitée du 24 octobre 1995 doit être l'occasion de lever toutes les ambiguïtés sur l'applicabilité du droit européen de la protection de la vie privée et des données personnelles à des acteurs de l'Internet établis hors de l'Union européenne. La Commission européenne semble d'ailleurs partager ce constat, puisque, dans sa communication précitée du 4 novembre 2010, elle « *considère que même si le traitement des données à caractère personnel est confié à un responsable établi dans un pays tiers, les intéressés doivent pouvoir bénéficier de la protection à laquelle ils ont droit en vertu de la Charte des droits fondamentaux de l'Union européenne et de la législation de l'Union européenne en matière de protection des données* ».

C'est pourquoi, la mission propose que, dans le cadre de la révision de la directive du 24 octobre 1995, les règles relatives au droit applicable soient clarifiées et précisées, afin d'assurer le même niveau de protection de la vie privée et des données personnelles à tous les résidents de l'Union européenne, indépendamment du lieu d'établissement du responsable du traitement. Il conviendrait, pour ce faire, de soumettre tous les responsables de traitement, où qu'ils se trouvent et même s'ils sont établis hors de l'Union européenne, aux juridictions et au droit des États membres dès lors qu'ils visent les publics qui y résident.

Comme le rappelle d'ailleurs M. Christian Cointat, dans son rapport précité sur la proposition de loi de M. Yves Détraigne et Mme Anne-Marie Escoffier, une évolution en ce sens de la directive du 24 octobre 1995 *« serait conforme au principe de réciprocité. En effet, lorsqu'un site Internet, implanté en Europe, porte atteinte à la protection de données de résidents américains, par exemple, sur le fondement de la loi de protection des mineurs votée en 1998 - Children's Online Privacy Protection Act, les juridictions américaines se déclarent compétentes et appliquent leur droit national* » [(1)].

Orientation n° 31 : mettre fin aux difficultés liées à l'extraterritorialité du droit applicable en matière de protection des données

Dans le cadre de la révision de la directive du 24 octobre 1995, assurer le même niveau de protection de la vie privée et des données personnelles à tous les résidents de l'Union européenne, indépendamment du lieu d'établissement du responsable du traitement.

Soumettre, pour ce faire, tous les responsables de traitement, où qu'ils se trouvent et même s'ils sont établis hors de l'Union européenne, aux juridictions et au droit des États membres dès lors qu'ils visent les publics qui y résident.

(1) Rapport n° 330, session ordinaire 2009-2010, de M. Christian Cointat, op. cit.*, p. 24.*

3. Vers un instrument juridique international de protection de la vie privée et des données personnelles ?

Cependant, la résolution des difficultés liées à la détermination du droit applicable ne saurait remédier à l'absence précédemment évoquée de cadre juridique international contraignant en matière de protection de la vie privée. Dans ce domaine, tout reste à inventer.

C'est pourquoi, la mission a, tout au long de ses travaux, accordé une importance toute particulière aux aspects européens et internationaux de la protection de la vie privée dans l'univers numérique.

Ainsi, la mission a organisé par visioconférence, le 19 janvier 2011, une réunion commune avec la commission d'enquête du *Bundestag* sur « Internet et la société numérique ». À l'issue de cette initiative parlementaire franco-allemande, sans précédent sur un tel sujet, une déclaration commune a été adoptée par la mission d'information et la commission d'enquête du *Bundestag*. Cette déclaration, qui figure en annexe [(1)], souligne notamment que « *l'élaboration d'instruments internationaux, allant au-delà du cadre européen, s'impose afin de permettre de mieux faire respecter la protection des droits de la personne* ».

Les jalons d'une protection universelle de la vie privée ont d'ores et déjà été posés. La « résolution de Madrid » [(2)], adoptée par près de quatre-vingts autorités de protection des données, le 5 novembre 2009, à l'occasion de la Conférence internationale des autorités de protection de la vie privée, a défini les principes tendant à renforcer le caractère universel du droit à la protection de la vie privée et des données personnelles de tous les citoyens. Cette résolution préconise, notamment, l'élaboration d'une Convention universelle pour la protection des personnes à l'égard du traitement des données personnelles.

Lors de cette conférence de Madrid, une première ébauche du contenu des standards internationaux sur la protection des données personnelles et de la vie privée a ainsi été réalisée. Comme le souligne M. Christian Cointat, « *il s'agit d'un premier pas historique car cette conférence mondiale est parvenue à élaborer un corpus de règles communes adaptées aux dernières évolutions technologiques : les grands principes de protection des données, les droits dont bénéficient les individus, les obligations incombant aux responsables de traitement, les procédures internes à mettre en place au sein des entreprises et administrations à l'échelle mondiale* » [(3)].

Il appartient désormais aux pouvoirs publics des États considérés, et non aux autorités de contrôle, de réfléchir à la nécessité de mettre en œuvre le processus d'adoption d'une telle convention internationale. Cela risque de prendre

---

(1) Cf. annexe n° 2.

(2) Résolution sur l'urgence de protéger la vie privée dans un monde sans frontière et l'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles (cf. annexe 3).

(3) Rapport n° 330, session ordinaire 2009-2010, op. cit.*, p. 25.*

beaucoup de temps. Or nous n'avons plus le temps d'attendre. Il est, à cet égard, regrettable que le *e*-G8, qui s'est tenu à Paris les 24 et 25 mai 2011, n'ait pas permis d'y parvenir [(1)].

Aussi la mission appelle-t-elle de ses vœux une intensification de l'action diplomatique conjointe de la France et de l'Union européenne en vue de parvenir, à moyen terme, à l'adoption, sous l'égide des Nations unies, d'une convention internationale ayant force juridique contraignante sur la protection de la vie privée et des données personnelles.

La réussite d'une telle entreprise nécessite également qu'à court terme, les Parlements nationaux s'emparent de la question. Or, la mission observe que de nombreuses initiatives parlementaires sont actuellement en cours et notamment qu'en application de l'article 34-1 de la Constitution, à l'Assemblée nationale comme au Sénat, ont été déposées deux propositions de résolution visant à soutenir la signature d'une telle convention universelle [(2)]. Aussi la mission apporte-t-elle tout son soutien à ces propositions de résolution, dont elle souhaite qu'elles puissent être rapidement examinées et adoptées dans chacune des chambres.

Orientation n° 32 : une action diplomatique forte pour l'adoption d'une convention internationale en matière de protection de la vie privée

À court terme, adopter au Parlement français, en application de l'article 34-1 de la Constitution, une résolution visant à soutenir la signature d'une convention internationale sur la protection de la vie privée et des données personnelles.

À moyen terme, promouvoir par l'action diplomatique conjointe de la France et de l'Union européenne l'adoption d'une convention internationale sous l'égide de l'ONU relative à la protection de la vie privée et des données personnelles.

*
* *

La vie privée et sa protection constituent donc un enjeu fondamental, qui sera, dans les mois et années à venir, d'autant plus incontournable dans le débat public que les individus se montrent aujourd'hui de plus en plus sensibles à la confidentialité et à la sécurité de leurs données personnelles sur Internet. En effet, en permettant le développement continu de services toujours plus innovants,

*(1) Lors de l'*e*-G8, aucun régulateur des données personnelles et de la vie privée, ni aucune association de défense des libertés ou des consommateurs n'était présent et seul un atelier «* Le dilemme des données : la vie privée dans un monde de réseaux *» était consacré au respect de la vie privée dans la révolution numérique.*

(2) Proposition de résolution visant à apporter le soutien de l'Assemblée nationale à l'élaboration d'une convention internationale relative à la protection de la vie privée et des données personnelles (n° 2837 – octobre 2010) ; proposition de résolution visant à apporter le soutien du Sénat à la signature d'une convention universelle pour la protection des personnes à l'égard du traitement des données personnelles (n° 168 – décembre 2010).

le Web 2.0 a parfois relégué au second plan la sécurité des échanges. Comment Internet pourra-t-il poursuivre son spectaculaire développement tout en offrant aux individus un haut niveau de sécurité des données échangées chaque jour sur la « Toile » ?

DEUXIÈME PARTIE : LA SÉCURITÉ DES ÉCHANGES DE DONNÉES SUR LES RÉSEAUX : UNE GARANTIE NÉCESSAIRE

I. UNE SITUATION MARQUÉE PAR DES MENACES PERMANENTES

A. LA NATURE DES MENACES PESANT SUR LA SÉCURITÉ DES ÉCHANGES

Outil d'une convivialité nouvelle, instrument d'enrichissement culturel, moyen de diffusion de nouveaux produits de consommation, Internet est conçu pour des relations d'échanges marquées par la confiance. Mais tout système sur lequel on peut interagir présente des failles de sécurité, comme a pu le rappeler M. Fabrice Le Fessant, chargé d'enseignement à l'École polytechnique [(1)]. Parmi les menaces qui pèsent en permanence sur cet outil de communication, les plus lourdes sont celles qui mettent en péril les droits de l'individu en visant la confidentialité de ses données personnelles. Cette situation conduit à formuler des exigences de sécurité qui soient à la hauteur des risques encourus par les personnes concernées.

Selon M. Patrick Pailloux, directeur général de l'agence nationale de la sécurité des systèmes d'information (ANSSI) [(2)], les attaques informatiques se distinguent des autres types d'agressions en ce qu'elles sont faciles à réaliser - elles sont très peu onéreuses et sont pratiquement invisibles – et qu'elles présentent un risque très faible pour l'agresseur. L'attaque informatique est ainsi dissymétrique par nature.

De plus, à la différence du domaine militaire classique où les États développent des armements et en empêchent la prolifération, les armes utilisées sont conçues par des membres du cyberespace et mises à la disposition du plus grand nombre. Les efforts faits par les États pour mettre en place des systèmes antiprolifération sont donc voués à l'échec.

La capacité de nuisance de ces détournements informatiques est telle que des conflits entre États se déroulent en parallèle sur les réseaux : l'Estonie, en 2007 ; la Corée du Sud, victime de nombreuses agressions informatiques dans le cadre du conflit qui l'oppose à la Corée du Nord ; l'Inde et le Pakistan, s'accusant d'attaques informatiques visant leurs diplomates ; le conflit israélo-palestinien, qui donne sans arrêt lieu à de telles attaques. Le Groupe d'experts intergouvernemental sur l'évolution du climat a, quant à lui, été victime d'un piratage de ses courriels dans un but politique. Cette guerre numérique s'étend aux conflits internes aux États ; les mouvements de révoltes politiques qui ont

(1) Audition du 5 mai 2010.
(2) Audition du 16 novembre 2010.

récemment touché le monde arabe ont montré quels pouvaient être les enjeux d'une maîtrise technique du réseau numérique.

Les techniques d'espionnage informatique sont de plus en plus sophistiquées : la plus répandue consiste à introduire sur l'ordinateur ciblé un logiciel espion qui prend le contrôle du terminal, vole les fichiers qui y sont contenus, enregistre ce qui est tapé au clavier, voire active le microphone ou la caméra du poste espionné.

Le ver informatique *Conficker* a infecté, en 2009, un très grand nombre de systèmes informatiques En 2010, un ver baptisé *Stuxnet* a pris pour cible des systèmes de « commande-contrôle » industriels utilisés, entre autres, dans la distribution électrique, les transports en commun, les systèmes ferroviaires, les contrôles aériens et la distribution d'eau.

En mai 2011, la firme Sony a annoncé avoir été victime d'un piratage informatique qui a conduit au vol des données personnelles et probablement des numéros de cartes bancaires de 77 millions de détenteur de comptes de son service de jeux vidéo en ligne.

La création de réseaux entiers d'ordinateurs – parfois plusieurs centaines de milliers de postes informatiques – tous infectés par le même virus et contrôlés à distance, représente une menace particulièrement redoutable. Permettant la gestion d'importants flux d'informations dans des buts criminels, ces réseaux de robots, appelés « *botnets* », constituent des outils efficaces pour rendre indisponible un site informatique ou procéder à des vols de données. L'une des caractéristiques de cette technique est que les propriétaires des ordinateurs corrompus ignorent que leur ordinateur a été transformé en instrument de piratage.

Les attaques contre les postes informatiques des particuliers sont si fréquentes que plus d'un tiers des internautes européens en auraient été victimes en 2010 [(1)]. Les procédés d'hameçonnage, consistant à soutirer à la victime des données personnelles en lui faisant croire qu'elle s'adresse à un tiers de confiance, sont d'un usage très répandu ; l'ANSSI a fait fermer 1 500 sites spécialisés dans cette technique en 2009.

Le développement des communications électroniques sans fil fragilise également la sécurité des transferts de données. M. Thomas Clausen, maître de conférences à l'École Polytechnique [(2)], a ainsi expliqué devant la mission d'information qu'il était facile de « casser » un réseau Wifi et de prendre connaissance du contenu de courriels. Pour preuve, on sait que les prises d'images effectuées par *Google Street View* ont donné lieu, en parallèle, à la collecte de données de connexion et de données personnelles, ce qui a suscité une très vive émotion.

---

(1) Selon une enquête menée par l'office statistique de l'Union européenne (Eurostat). http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF

(2) Audition du 5 mai 2010.

M. Patrick Pailloux a souligné l'inquiétude constante qui était la sienne, au regard de ses responsabilités, face aux menaces de piratage. Cette inquiétude s'est révélée justifiée puisqu'en mars 2011, en France, le ministère de l'Économie et des finances a révélé avoir été l'objet d'un piratage. Les postes informatiques avaient été infiltrés par le biais de leur messagerie ; les services de la présidence de la République ainsi que ceux du ministère des Affaires étrangères auraient, eux aussi, été touchés.

Si la vigilance des experts doit être permanente, il est cependant difficile d'anticiper les attaques informatiques ; comme l'a précisé M. Sylvain Thiry [(1)], responsable de la sécurité des systèmes d'information de la SNCF, un système de sécurité informatique ne peut être qu'en position de réaction face aux menaces.

Les craintes que suscite la sécurité des réseaux sont telles qu'elles ont été évoquées par les chefs d'État et de gouvernement du G8, réunis à Deauville les 26 et 27 mai 2011 : « *Le fait que l'Internet puisse être utilisé à des fins contraires aux objectifs de paix et de sécurité et porter atteinte à l'intégrité des systèmes d'importance critique, demeure une source de préoccupation.* » [(2)] Le danger que représente la constitution de réseaux d'ordinateurs contrôlés à distance dans des buts malveillants a été en particulier souligné.

B. L'ACTION DE L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

La multiplicité des menaces pesant sur les réseaux informatiques et les risques de voir entravé le bon fonctionnement de l'État ont rendu indispensable la création d'un organisme national apte à engager des procédures unifiées de sécurisation. A été ainsi créée en 2009 [(3)], l'Agence nationale de la sécurité des systèmes d'information, service à compétence nationale, rattaché au secrétaire général de la défense et de la sécurité nationale.

L'agence est chargée de proposer des règles de sécurité tant pour les systèmes d'information des autorités publiques que pour les « opérateurs d'importance vitale » [(4)]. Elle assure un service de veille, de détection, d'alerte et de réactions aux attaques informatiques. L'inspection des systèmes informatiques des services de l'État ainsi que la formation des personnels qualifiés dans ce domaine relèvent également de sa compétence.

En collaboration avec l'Agence européenne de sécurité de l'information et des réseaux (ENISA), l'ANSSI participe à des exercices paneuropéens de défense contre les cyberattaques.

---

(1) Audition du 19 octobre 2010.
(2) Déclaration du G8 de Deauville, 26-27 mai 2011, § 17.
(3) Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé : « Agence nationale de la sécurité des systèmes d'information ».
(4) Cf. article 3 du décret précité.

Dans le cadre de ses missions, l'ANSSI a mis en place un référentiel général de sécurité. Ce document public peut également inspirer les services de sécurité informatique du secteur privé.

L'agence dispose d'un centre opérationnel des systèmes d'information (COSSI) qui fonctionne en continu pour apporter, en cas de faille de sécurité, une aide technique aux différents services informatiques de l'État. Elle enregistre ainsi plusieurs centaines d'incidents de sécurité chaque année.

Dépendant de l'ANSSI, le Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA) contribue à la bonne information des acteurs de la sécurité informatique en mettant en ligne des alertes informatiques et des bulletins d'actualité d'une très grande précision technique [(1)]. Des notes d'information pratique sont également diffusées par cet organisme.

L'ANSSI a, en outre, créé un portail officiel de la sécurité informatique [(2)] qui dispense des conseils aux particuliers et aux entreprises et émet des bulletins d'alerte.

Enfin, l'ANSSI se prononce sur la sécurité des dispositifs et des services offerts par les prestataires privés. Elle certifie, notamment, les dispositifs de création et de vérification des signatures électroniques, délivre des autorisations et assure la gestion des déclarations relatives aux moyens et prestations de cryptologie.

M. Patrick Pailloux a souligné que les moyens humains de l'agence qu'il dirige sont, certes, en progression – étant passés de 110 à 250 employés – mais qu'ils restent deux fois inférieurs aux organismes homologues existant en Allemagne et en Angleterre.

CRYPTOLOGIE ET SIGNATURE ÉLECTRONIQUE

La cryptologie

Rendre secret le contenu d'une information pour en réserver la lecture à des destinataires choisis semble être le meilleur moyen de sécuriser un échange de données. La fiabilité d'un cryptage dépend de la complexité du chiffrage employé.

Cette technique n'est pas réservée aux communications dites « sensibles » de l'État. Elle est utilisée pour les paiements en ligne et pour les communications audiovisuelles en ligne transitant par le logiciel Skype. Elle peut l'être aussi par des cybercriminels.

La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, dans son article 30, a libéralisé l'utilisation des moyens de cryptologie. La fourniture de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité demeure néanmoins soumise à un régime de déclaration ou d'autorisation en cas de transfert de la technologie à l'étranger.

(1) Cf. http://www.certa.ssi.gouv.fr/site/index_act.html.
(2) Cf.http://www.securite-informatique.gouv.fr/

L'utilisation de la cryptologie est limitée par son coup économique : plus le niveau de chiffrage est élevé, plus les ordinateurs utilisés doivent être puissants.

La multiplication de données cryptées peut aussi avoir pour conséquence un ralentissement de la vitesse des échanges, le déchiffrage exigeant du temps.

Les solutions techniques sont encore à trouver pour rendre compatibles les contraintes techniques propres à la cryptologie avec le développement de l'externalisation massive des données dans le cadre du cloud computing.

La signature électronique

La signature électronique a pour finalité d'apporter à l'utilisateur un moyen de s'authentifier, de manière sécurisée, pour accéder à un service en ligne et signer par voie électronique un document. La procédure doit également garantir l'intégrité du document.

Le but de cette technique est d'écarter le risque d'usurpation d'identité et de falsification du document.

L'identité du signataire est enregistrée sur une puce cryptée (pouvant être hébergée sur une clé USB) selon le principe de la cryptographie asymétrique associant une clé privée et une clé publique. Le message chiffré par une clé ne peut être lu que par l'autre. L'opération n'est pas symétrique en ce que chaque clé n'a pas une fonction identique à l'autre mais inverse : l'une chiffre, l'autre déchiffre. La clé publique est mise à disposition d'un ensemble d'utilisateurs, la clé privée est réservée à un seul individu.

L'accès à l'identité se fait par un mot de passe.

La réussite du décodage prouve que la clé est celle qui fait la paire avec celle de chiffrement. Encore faut-il s'assurer de l'identité de la personne qui se présente comme étant le titulaire de celle-ci. Une autorité de certification est nécessaire ; sa fonction est de servir de tiers de confiance garantissant le lien entre la personne morale ou physique et l'identité de la clé numérique. La procédure est ainsi liée à la possession par le signataire d'un certificat numérique.

Les autorités de certification font l'objet d'un agrément, par exemple par le ministère de l'Économie, des finances et de l'industrie pour les candidats à des marchés publics.

La légalisation de la signature électronique remonte à l'adoption de la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique mais le premier acte authentique notarial n'a été signé par ce moyen qu'en 2008. Quelques services bancaires ont recours à cette technique qui s'est systématisée depuis le 1er janvier 2010 dans le cadre de la dématérialisation des marchés publics.

Le projet de carte d'identité électronique prévoit que celle-ci contiendra, en plus des données biométriques numérisées, un service d'authentification à distance et de signature électronique. Cette fonctionnalité est déjà présente sur la carte d'identité électronique belge.

II. ASSURER PLUS DE TRANSPARENCE EN CAS DE FAILLES DE SÉCURITÉ

L'internaute est impuissant face aux attaques informatiques ; il en est réduit à espérer que les logiciels de protection vendus sur le marché le protégeront d'au moins une partie des risques auxquels il s'expose dès qu'il se connecte au

réseau. Mais l'intérêt en jeu est beaucoup plus large dans le cas de la sécurité de réseaux entiers, en particulier lorsqu'y sont hébergées des bases contenant des données personnelles. Au regard des conséquences que peuvent avoir des failles de sécurité, les personnes concernées doivent pouvoir compter sur des procédures transparentes d'information.

A. LES OBLIGATIONS DE SÉCURITÉ

1. Les services de communication électronique

La transposition du « paquet télécoms » va renforcer les exigences de sécurité pesant sur les opérateurs de communications électronique. Le Parlement européen demande en effet aux États membres d'adopter des mesures susceptibles de garantir un niveau de sécurité adapté au risque existant (1). Deux dispositions devraient ainsi être introduites : la première permettra aux États d'imposer des normes portant sur l'intégrité et la sécurité des réseaux ; la seconde visera à soumettre les opérateurs à des contrôles de sécurité effectués par un organisme qualifié indépendant.

2. L'administration électronique

L'organisation de la sécurité des échanges électroniques entre les administrations et entre l'administration et les administrés s'appuie, depuis 2010, sur un référentiel général de sécurité (2). À considérer les propos introductifs de la version 1.0 de ce référentiel, l'instauration de ces normes répondait à une situation d'urgence : « *La sécurité des technologies de l'information n'a pas suivi l'extraordinaire développement de l'informatique et de ses usages. Le protocole Internet – l'IP –, les systèmes d'exploitation et les applications ont à l'origine été conçus pour être efficaces dans des réseaux peu étendus, sans réelle prise en compte de la sécurité. Ceux qui sont aujourd'hui en service utilisent souvent des briques de base des premiers réseaux, alors que leur contexte d'emploi a radicalement changé, avec la multiplication des technologies de communication (notamment dans le domaine du « sans fil »), la convergence des réseaux de téléphonie, de messagerie ou de transmissions de données vers l'Internet et l'interconnexion de ces réseaux. Les logiciels, de plus en plus complexes, présentent souvent des failles de sécurité, qui obligent les éditeurs à les corriger en permanence, dès leur découverte. Les informations, hier confinées, sont devenues accessibles depuis presque n'importe quel point du globe, alors que dans le même temps, leur volume explose avec l'augmentation du nombre de*

(1) Cf. article 1er de la directive 2009/140/CE modifiant les articles 13 bis *et 13* ter *de la directive 2002/21/CE.*

(2) Décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9,10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives en entre les autorités administratives.

processus dématérialisés d'une part et des capacités de calcul et de stockage d'autre part. » (1)

Le référentiel général de sécurité définit quatre fonctions de sécurité :

– **l'identification**, à savoir les procédés techniques utilisés pour vérifier l'identité de l'usager ;

– **la signature électronique** : elle doit garantir l'identité du signataire et l'intégrité du document ;

– **la confidentialité** : elle apporte l'assurance qu'une information ne peut être consultée par un tiers non autorisé au cours de son transfert ou de son stockage ;

– **l'horodatage**, qui est la trace dans le temps de l'existence d'un document ; l'horodatage est un élément de preuve dans les échanges électroniques.

Le référentiel prévoit également que son contenu ainsi que l'évaluation des besoins de sécurité de chaque autorité administrative devront prendre en compte l'évolution des technologies. Comme le souligne la directive du Parlement européen du 25 novembre 2009, « *l'application fructueuse de mesures de sécurité appropriées n'est pas un exercice effectué une fois pour toutes, mais un processus continu de mise en œuvre, de réexamen et d'actualisation.* » (2) Différentes versions du référentiel de sécurité sont donc à attendre.

Par ailleurs, l'ANSSI est habilitée à attribuer des labels qui garantissent la conformité des produits de sécurité et des prestataires de service aux critères du référentiel général de sécurité. Ce dispositif constitue un élément de diffusion des bonnes pratiques pour l'ensemble du secteur privé.

3. Les bases de données

Concernant plus particulièrement la sécurité des bases de données personnelles, l'article 17 de la directive 95/46/CE (3) dispose que « *Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer,*

(1) Version 1.0 du 6 mai 2010, approuvée par arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques : http://references.modernisation.gouv.fr/sites/default/files/RGSv1.0.pdf.

(2) Cf. directive 2009/140/ CE du 25 novembre 2009, considérant 44.

(3) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. »

En droit interne, aux termes de l'article 34 de la loi du 6 février 1978, une obligation de moyens pèse sur le responsable du traitement, lequel *« est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* » La violation de cette obligation est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende conformément à l'article 226-17 du code pénal.

En matière de sécurité, parmi les formalités de déclaration d'une base de données personnelles, la CNIL interroge le responsable de traitement sur les points suivants : la protection de l'accès physique au local contenant les fichiers ; la mise en œuvre de procédés d'identification des utilisateurs (par exemple mot de passe individuel, carte à puce, certificat, signature) ; l'enregistrement des utilisations dans un journal des connexions ; la localisation de la base sur un réseau interne non relié à Internet ; les caractéristiques du canal de transport utilisé et l'éventuel recours au chiffrage si les données sont échangées. Les contrôles exercés sur place par la CNIL permettent de s'assurer du caractère réel des mesures de sécurité mises en œuvre.

B. LES PROCÉDURES EN CAS DE FAILLES DE SÉCURITÉ

Si le nombre de failles de sécurité et la quantité de données personnelles concernées sont difficiles à chiffrer, le phénomène est incontestablement important. Une enquête a été réalisée aux États-Unis portant sur un ensemble de failles qui aurait touché, en 2010, près de 900 millions de données [(1)]. La prise en compte par les législations de 46 États américains sur 50 des conséquences juridiques de ces situations atteste de l'ampleur du phénomène [(2)] de même que le montant des amendes infligées – 375 000 dollars, en 2010, pour la société américaine D.A. Davidson and Co [(3)]. Au Royaume-Uni, en 2009, l'autorité des services financiers [(4)] a prononcé une amende de 3 millions de livres à l'encontre de trois organismes de la banque HSBC qui n'avaient pas respecté des procédures de sécurité suffisamment rigoureuses dans la gestion des données informatiques de leurs clients – amende importante en valeur absolue mais de faible portée au regard du chiffre d'affaires de la société.

---

(1) Cf. Verizon Data Breach Investigations Report*, édition 2010. http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.*

(2) Cf. http://www.ncsl.org/default.aspx?tabid=13489.

(3) L'autorité américaine de régulation de l'industrie financière (FINRA) a jugé, le 12 avril 2010, que la société D.A. Davidson and Co. n'avait pas assuré un niveau de sécurité nécessaire à ses réseaux ce qui avait permis à des pirates de s'emparer de données personnelles de 192 000 personnes. http://www.finra.org/newsroom/newsreleases/2010/p121262.

(4) Financial Services Authority (FSA), juillet 2009.

Tout dernièrement, en France, la CNIL a infligé une amende de 100 000 euros à *Google* dans l'affaire *Google Street view* [1]. Dès 1981, la Cour de cassation avait pu confirmer une condamnation d'un montant de 50 000 francs prononcée contre le Syndicat interprofessionnel des médecins du travail du pays d'Aix (SIMTPA) pour avoir mis en place un système de gestion informatique des données médicales « *sans qu'aient été prises toutes les précautions utiles en vue d'empêcher la communication des informations médicales aux membres du personnel administratif.* » [2]

La crainte des préjudices que pourrait causer à l'image des entreprises concernées une politique d'information transparente en cas de faille de sécurité ne contribue pas à une évaluation objective du phénomène. Il semblerait même qu'au sein des entreprises, les services informatiques hésitent parfois à informer leur hiérarchie, ce qui ne facilite pas la prise de conscience de la nécessité d'investir dans des systèmes de sécurité.

Au silence des sociétés concernées s'ajoutent les craintes dues aux risques juridiques encourus par toute personne qui souhaiterait avertir le public de l'existence de ces failles. Si le défaut de sécurité fait l'objet d'une description suffisamment précise pour que toute personne qui en prend connaissance puisse à son tour exploiter la faille, la responsabilité pénale de l'auteur de l'information peut, en effet, être engagée. [3]

Une information rapide et transparente est pourtant indispensable. Elle permet, sur un plan technique, de lancer des alertes à l'ensemble des informaticiens gestionnaires de réseaux. M. Patrick Pailloux a ainsi regretté que de nombreux incidents ne soient pas spontanément déclarés à l'ANSSI.

Elle devrait surtout conduire à informer les personnes dont les données personnelles sont rendues publiques, ou, à tout le moins, l'organisme compétent en matière de protection des données. La mission d'information a ainsi appris, non sans surprise, que la CNIL n'avait eu connaissance que par la presse du piratage dont avait été victime, en mars 2010, le site *voyages-sncf.com.*

Si la loi n° 2004-801 du 6 août 2004 a créé la fonction de correspondant informatique et libertés (CIL) – on en compte, aujourd'hui, plus de deux mille en activité – encore faut-il que le CIL soit lui-même mis au courant du problème par le responsable du traitement. De plus, aux termes de l'article 45 du décret du 20 octobre 2005 [4] si le CIL a connaissance de l'existence de manquements avant le responsable de traitement, il doit en informer ce dernier avant toute saisine de la CNIL.

(1) Délibération 2011-035, 17 mars 2011.
(2) Cf. Cour de Cassation, chambre criminelle, 30 octobre 2001, n° 99-82136.
(3) Cf. Cour de Cassation, chambre criminelle, 27 octobre 2009, n° 09-82346 et article 323-3-1 du code pénal.
(4) Décret n° 2005-1309 du 20 octobre 2005.

De fait, aucune obligation légale précise ne s'impose au responsable de traitement, en dehors de l'obligation générale de sécurité posée à l'article 34 précité. Seul le guide de sécurité édité par la CNIL recommande au responsable de traitement d'informer les personnes concernées [1]. Mais ce n'est qu'une fois que le CIL constate que les manquements persistent qu'il lui est recommandé de prévenir la CNIL. Or on sait que la gravité d'une faille de sécurité ne dépend pas de sa durée. Un temps très bref suffit pour que des données personnelles soient recopiées et diffusées.

Comme il en a été fait mention dans le présent rapport, dans la partie consacrée à la vie privée [2], la future transposition du « paquet télécoms » devrait cependant conduire à améliorer la transparence de l'information tant du point de vue technique, lorsque la sécurité des réseaux est en jeu, que du point du droit des personnes, lorsque des données personnelles sont en cause.

Sur le premier aspect, la directive 2009/140/CE [3] dispose en effet, dans son article 13 *bis* que « *Les États membres veillent à ce que les entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public notifient à l'autorité réglementaire nationale compétente toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.* »

La transposition de cette directive devrait permettre à l'État d'imposer des normes de sécurité et d'obliger les opérateurs à faire contrôler leur réseau par des organismes indépendants. À cet égard, on ne peut que regretter que la voie des ordonnances ait été choisie au détriment d'un débat parlementaire qui aurait été très légitime sur une telle question.

Sur le second aspect, la directive 2009/136/CE [4], introduit, en son article 2, la disposition suivante : « *La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à l'autorité nationale compétente décrit*

(1) Cf guide : sécurité des données personnelles, fiche n°8, traçabilité et gestion des incidents, éd.2010., CNIL. http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite%20VD.pdf.

(2) Cf. II de la première partie du titre II du présent rapport.

(3) Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.

(4) Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier ».

Les conséquences négatives visées dans le texte sont *« par exemple, le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique, une humiliation grave ou une réputation entachée* […]. » (1)

Le projet d'ordonnance transposant ces deux directives en droit interne prévoit ainsi, en cas de violation de données personnelles, l'information sans délai de la CNIL et des personnes intéressées, la rapidité de l'information étant la condition nécessaire pour assurer la transparence de la procédure.

En l'état des textes, ces dispositions ne s'imposent cependant qu'aux opérateurs de service de communications électroniques et non aux fournisseurs de contenus. Leur portée s'en trouve donc considérablement limitée. La directive 2009/136/CE en appelle d'ailleurs, dans son considérant 59, à une extension du dispositif pour que celui-ci soit applicable « *quel que soit le secteur ou le type de données concerné »,* la Commission devant promouvoir, « *sans retard* » les mesures correspondantes.

Face au processus d'accumulation massive de données auquel on assiste aujourd'hui et constatant la multiplication des failles de sécurité, la mission d'information partage ce sentiment d'urgence. Les personnes dont les données personnelles sont devenues publiques doivent pouvoir faire valoir leurs droits à réparation.

Dans l'orientation n° 25 du présent rapport les rapporteurs ont exprimé le souhait qu'au-delà de cette transposition, des mesures plus contraignantes soient envisagées qui feraient peser les obligations de notification et d'information en cas de faille sécurité également sur les fournisseurs de contenus, voire sur tout détenteur d'une base de données personnelles déclarée à la CNIL comme il en va dans les législations de certains États des États-Unis – proposition qui figure par ailleurs à l'article 7 de la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, adoptée par le Sénat le 23 mars 2010 (2).

Au point de vue technique, il conviendrait d'assurer une plus grande transparence dans la communication des failles de sécurité, gage d'une meilleure réactivité de l'ensemble des acteurs concernés.

Le périmètre d'application de telles mesures demandera néanmoins à être évalué ; il ne faudrait pas que les organismes de contrôle soient submergés par des notifications de failles de sécurité très mineures, comme l'a fait remarquer M. Patrick Pailloux à propos de l'ANSSI. De même, l'information personnelle de

(1) Directive 2009/136/CE , considérant 61.

(2) Proposition de loi de M. Yves Détraigne et Mme Anne-Marie Escoffier visant à mieux garantir le droit à la vie privée à l'heure du numérique*, n°93 (2009-2010).*

toutes les personnes concernées par une faille de sécurité risque, dans certains cas, de se révéler disproportionnée ou non réalisable.

Orientation n° 33 : renforcer les procédures d'information en cas de faille de sécurité

Mettre en place un dispositif d'information de l'Agence nationale de la sécurité des systèmes d'information en cas de faille de sécurité importante sur un réseau informatique.

III. L'INFORMATIQUE DANS LES NUAGES : QUELLES GARANTIES POUR LA CONFIDENTIALITÉ DES DONNÉES PERSONNELLES ?

La mise en réseau des informations a d'abord été comprise comme la possibilité de faire communiquer des sources d'informations, qu'il s'agisse des internautes entre eux, de sociétés commerciales proposant des produits à des consommateurs ou de services publics s'adressant à des administrés. Depuis peu, l'idée de procéder à un niveau de partage plus profond est devenue techniquement réalisable : la gestion des données qui, jusqu'à présent, était effectuée par chaque acteur d'Internet pour son propre compte, peut se faire, elle aussi, sous la forme d'échanges, les données étant confiées à des prestataires qui les stockent et les gèrent à la commande.

Cette dissémination des données dans l'ensemble du nuage informatique est ce qui est appelé le « *cloud computing* » ou, en français, « informatique en nuage »[(1)]. Les données ne sont plus localisées ; elles circulent en permanence à l'intérieur de l'espace de communication d'Internet.

Les développeurs des techniques de « *cloud computing* » cherchent ainsi à tirer un bénéfice économique de la rapidité et de la souplesse des échanges qui caractérisent Internet, faisant valoir qu'une exploitation de données réalisée en partage sur le réseau diminue considérablement leur coût de gestion.

La promotion de ce mode de gestion suscite cependant des interrogations. Quel est le degré de protection des données pendant et après leur transfert ? Que deviennent les données lorsque le prestataire fait défaut, par exemple en cas de faillite ? Dans quelle mesure le prestataire peut-il sous-traiter la base de données qui lui a été confiée ? Dans le cas de déterritorialisations en cascades, quelle législation s'applique ? Quelles garanties y a-t-il que les données ne sont pas dupliquées ou corrompues ? Où les données, traitées par des serveurs mis en réseau, sont-elles précisément localisées à un instant « t » ? À l'intérieur de cet immense flux d'informations, comment les données personnelles sont-elles distinguées des autres ?

(1) Terminologie fixée au Journal Officiel du 26 juin 2010.

Enfin, dans un contexte technique très évolutif, quelles garanties le client a-t-il que la base de données qu'il externalise sera gérée, à tous les stades de la chaîne de sous-traitance, dans des formats informatiques compatibles avec ceux qu'il utilise ?

A. UNE NOUVELLE ÉTAPE DANS LE DÉVELOPPEMENT DES POTENTIALITÉS DES RÉSEAUX

De plus en plus de sociétés commerciales n'hébergent plus leurs données sur des serveurs localisés dans les mêmes lieux physiques que leurs unités de gestion mais les confient, par le biais du réseau, à des prestataires qui les stockent dans des centres de données (*data centers*) pouvant être localisés n'importe où dans le monde.

LES *DATA CENTERS*

L'externalisation de la gestion informatique des données conduit à multiplier le nombre de serveurs accessibles en ligne. La construction de nouveaux centres d'hébergement de données (*data centers*) est ainsi stimulée par le développement du cloud computing.

Google disposerait de 36 *data centers*, contenant plus de 200 000 serveurs, et *Facebook* en gérerait 9.

Les bâtiments dans lesquels sont stockés les serveurs ont une surface moyenne variant entre 10 000 et 20 000 mètres carrés. Le nouveau *data center* d'*Apple*, en Caroline du Nord, s'étendra sur 48 000 mètres carrés. En France, France Télécom Orange construit un centre d'hébergement à Val-de-Reuil qui aura une superficie de 16 000 mètres carrés et IBM un centre de 10 000 mètres carrés à Seclin, dans la banlieue lilloise.

La gestion de *data centers* passe par des mesures de sécurité très strictes destinées à garantir la bonne conservation des informations stockées : sécurité de l'accès physique ; sécurité contre les incendies ; redondance des alimentations électriques et des infrastructures critiques ; climatisation garantissant une température et un taux d'humidité constant ; service assuré en continu.

La maîtrise de la consommation électrique et la climatisation des espaces d'hébergement constituent les deux principales difficultés techniques pour la maintenance des *data centers*. Une meilleure prise en compte des facteurs environnementaux est mise en avant dans les projets les plus récents.

En Europe, le marché des *data centers* se développe actuellement au profit des pays du Nord où les dépenses d'énergie pour la climatisation sont moindres.

Ces concentrations de serveurs – on parle de « grappes de serveurs » ou de « ferme de calcul » – augmentent les capacités de traitement des données en ligne mais peuvent, dans certaines conditions, constituer un facteur de fragilisation d'Internet. Des pannes dans un *data center* font en effet courir le risque d'une paralysie de pans entiers du réseau.

Dans le *cloud computing*, l'hébergement de données n'est pas la seule prestation proposée ; des applications comptables, par exemple, sont développées pour être utilisées en ligne par le client. Le gain financier est important : les entreprises n'ont plus à investir dans l'achat, l'entretien et l'exploitation de supports informatiques coûteux et très sensibles à l'évolution des technologies.

L'environnement « collaboratif » spécifique du Web 2.0 profite de cette nouvelle division du travail. Sans avoir à installer sur son ordinateur les applications qui lui sont nécessaires, l'utilisateur dispose des outils dont il a besoin pour un usage réalisé directement sur des serveurs en réseau. Ce système permet en particulier de dégager des puissances de calcul très importantes.

Disposer des logiciels les plus performants sans en acheter les licences d'utilisation, avoir accès à des plateformes de services pour créer, à moindres frais, de nouvelles applications, déporter des données dans des espaces de stockage sécurisés en ligne, tels sont les trois fonctionnalités de base du *cloud computing* (1).

Pour accéder à l'ensemble de ces services, l'utilisateur n'a besoin que d'une connexion à Internet. Mais cette externalisation des actions a pour contrepartie que l'utilisateur n'a plus le contrôle de ses outils informatiques ni des données qu'il est amené à transférer sur la toile : le nuage informatique est complètement opaque.

Par ailleurs, si les gains économiques attendus du développement du *cloud computing* sont considérables, il convient de rester attentif au fait que les nombreuses campagnes de communication lancées sur ce thème ont surtout un but commercial, leurs promoteurs étant les grandes entreprises informatiques capables de vendre, précisément, ce type de service.

B. LE NUAGE INFORMATIQUE ET SES OMBRES

Le partage des données sur Internet signifie aussi l'interdépendance des acteurs. Le système du *cloud computing* suppose en effet la continuité du service assuré par les fournisseurs d'accès au réseau, la sécurité des échanges et la fiabilité des prestataires, ce dernier point posant la question du devenir des données personnelles en cas de sous-traitance en cascade.

1. Continuité du service et sécurité des échanges

La continuité du service renvoie aux questions de la neutralité du réseau, abordées précédemment.

Concernant la sécurité, en décembre 2010, l'ANSSI a formulé la mise en garde suivante : « *les offres d'informatique en nuage public ne donnent généralement pas des garanties suffisantes pour la sécurité* » (2).

Selon l'ANSSI, trois catégories de risques sont à prendre en compte. La première est la perte de maîtrise du système d'information, lorsque le lien entre l'organisme fournissant les données et celui qui les traite se distend ou se rompt,

(1) Ces fonctions sont identifiées par les acronymes suivants : SaaS (Software as a Service), PaaS (Platform as a Service) et IaaS (Infrastructure as a Service).

(2) ANSSI, communiqué de presse du 3 décembre 2010.

soit parce qu'il y a eu sous-traitance en cascades, soit parce que la localisation des données n'est pas maîtrisée, soit encore en raison des choix techniques du prestataire influant sur l'interopérabilité ou la sécurité des systèmes. La deuxième catégorie de risques provient du fait que les interventions se font en ligne, à distance, ce qui augmente les risques d'intrusion ou d'abus de droits. Le dernier groupe de risques est lié à l'hébergement mutualisé qui favorise la propagation des incidents.

L'ANSSI a donc édité un guide (1) expliquant les obligations contractuelles qu'il est souhaitable d'imposer aux prestataires au regard de ces trois catégories de risques. Il y est en particulier rappelé que l'externalisation de la gestion de données personnelles fait l'objet de dispositions de la part de la CNIL.

2. Les données personnelles dans le *cloud computing*

L'externalisation de données personnelles peut être motivée, par exemple, par le souhait de centraliser, à l'intérieur d'un groupe international, des bases de données portant sur la gestion des commandes, sur la comptabilité clients ou sur les ressources humaines. Il peut s'agir aussi d'un transfert vers un prestataire aux fins de saisie informatique de dossiers manuels ou dans le but de créer un centre d'appel à l'étranger.

La CNIL a rappelé, en 2008, les conditions légales des transferts de données à caractère personnel vers des pays non-membres de l'Union européenne (2).

L'analyse juridique de la légalité du transfert de données est complexe. Elle doit prendre en compte les principes généraux suivants :

« – Le traitement doit avoir régulièrement fait l'objet des formalités préalables requises par la loi : la CNIL ne saurait autoriser un transfert de données dès lors que le traitement original dont les données sont issues n'aurait pas été déclaré ou autorisé.

« – Tout transfert de données vers l'étranger doit avoir une finalité déterminée, explicite et légitime : le responsable de traitement établi en France doit pouvoir expliquer pourquoi le transfert a lieu et s'être assuré que ces raisons sont compatibles avec les exigences de la loi française.

« – Les données transférées ne doivent pas être traitées ultérieurement de manière incompatible avec cette finalité : le responsable de traitement doit pouvoir établir que la raison pour laquelle les données sont transférées est compatible avec les raisons pour lesquelles les données ont été initialement collectées.

(1) Cf. http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf.
(2) Cf. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf

« – Les données transférées doivent être adéquates, pertinentes et non excessives au regard de la ou des finalités pour lesquelles elles sont transférées » (1).

Concernant l'information des personnes concernées, celle-ci est obligatoire quand le transfert se fait en direction d'un pays non-membre de l'Union européenne (2).

Les manquements aux règles de transfert sont sanctionnés par cinq ans d'emprisonnement et 300 000 euros d'amende (3). Dans son programme d'action pour 2011, la CNIL a décidé de multiplier les contrôles dans ce secteur.

a) Les procédures légales d'exportation de données personnelles

Trois groupes de procédures sont à distinguer au regard des articles 25 et 26 de la directive 95/46/CE du 24 octobre 1995 et des articles 68 et 69 de la loi 78-17 du 6 janvier 1978.

– La Commission européenne peut prendre une décision « d'adéquation » par laquelle elle reconnaît que le pays vers lequel sont exportées des données personnelles assure un niveau de protection adéquat ou suffisant de la vie privée et des libertés et droits fondamentaux. La liste des pays bénéficiant de cette reconnaissance est la suivante : Andorre, Argentine, Australie, Canada, Suisse, les Îles Féroé, Guernesey, Israël, l'Île de Man et Jersey (4).

Les entreprises localisées aux États-Unis et adhérant aux règles des principes de la « sphère de sécurité » (*Safe Harbor*) sont alignées sur celles relevant de pays bénéficiant d'une décision d'adéquation (5).

Pour des transferts de cette nature, la CNIL n'a pas à donner d'autorisation. Seule une déclaration est nécessaire.

– Si le pays importateur des données ne bénéficie pas d'une telle reconnaissance, ou si l'entreprise destinataire n'adhère pas au *Safe Harbor*, il revient à l'autorité régulatrice, à savoir en France à la CNIL, de vérifier si les clauses contractuelles ou les règles internes de transfert, lorsqu'il s'agit d'une externalisation demeurant à l'intérieur d'un groupe international, présentent un degré suffisant de sûreté (6).

Les règles internes d'entreprise – *Binding corporate rules* (BCR) – définissent le cadre dans lequel s'effectuent les transferts des données personnelles

(1) Guide de transferts de données à caractère personnel vers des pays non membres de l'Union européenne, p. 8.
(2) Article 32 de loi n° 78-17 du 6 janvier 1978.
(3) Cf. articles 226-16, 226-16-1 A et 226-22-1 du code pénal.
(4) Cf. http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.
(5) Décision 2000/520/CE du 26 juillet 2000.
(6) Cf. article 69, al. 8, de la loi du 6 janvier1978.

depuis des filiales vers une maison mère située à l'étranger. Le G29 a adopté des lignes directrices concernant ce type d'externalisation.

Les clauses contractuelles ont été précisées par la Commission européenne en 2010, selon des modalités décrites ci-après.

L'autorisation donnée par la CNIL, pour ces deux types de transferts, est portée à la connaissance de la Commission européenne et des autorités européennes de contrôle.

– Enfin, ce dispositif est complété par un certain nombre d'exceptions décrites à l'article 69 de la loi du 6 janvier 1978 :

« Art. 69 : […] *le responsable d'un traitement peut transférer des données à caractère personnel vers un État ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :*

« 1° À la sauvegarde de la vie de cette personne ;

« 2° À la sauvegarde de l'intérêt public ;

« 3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;

« 4° À la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

« 5° À l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

« 6° À la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers. […] »

b) Les difficultés posées par les transferts de données personnelles sur des bases contractuelles

Le succès que connaît le *cloud computing* multiplie les cas de transferts de données sur des bases contractuelles. D'une part, en effet, il est de la nature même du *cloud computing* de procéder à des transferts de données en tout point du monde et donc majoritairement vers des pays extérieurs à l'Union européenne et ne bénéficiant pas de clauses de reconnaissance particulières. D'autre part, un intérêt économique pousse à opérer des externalisations de gestion de données vers des pays proposant des hébergements et des gestions à distance à des prix compétitifs.

Constatant l'intérêt grandissant pour la promotion des clauses contractuelles type, la Commission européenne a adopté, le 5 février 2010 une décision [1] qui précise les clauses qui peuvent être utilisées par un responsable du traitement de données établi dans l'Union européenne pour offrir des garanties adéquates au sens de l'art 26 de la directive précitée.

Ce texte, en vigueur depuis le 15 mai 2010, vise principalement à mieux encadrer les sous-traitances en cascades de manière à assurer une traçabilité juridique du statut des données dans la chaîne de contrats [2]. À cet effet, il encadre la liberté contractuelle en posant les principes suivants :

– Concernant la sécurité, les données à caractère personnel doivent être protégées contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement ;

– Pour assurer le respect du principe de la limitation des transferts à une finalité spécifique, énoncé dans la directive 95/46/CE, la sous-traitance ultérieure ne doit porter que sur les activités convenues dans le contrat conclu entre l'exportateur de données et l'importateur de données ; à tous les niveaux de sous-traitance, les contrats doivent intégrer les clauses contractuelles types et ne doivent pas avoir d'autres finalités ou concerner d'autres activités de traitement ;

– L'importateur devra traiter les données à caractère personnel pour le compte exclusif de l'exportateur de données et conformément aux instructions de ce dernier et aux clauses types ; s'il est dans l'incapacité de s'y conformer pour quelque raison que ce soit, il accepte d'informer dans les meilleurs délais l'exportateur de données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert de données ou de résilier le contrat ;

– En cas de sous-traitance ultérieure, l'importateur doit au préalable en informer l'exportateur de données et obtenir l'accord écrit de ce dernier. Cette clause donne de fait la faculté à l'exportateur de stopper la chaîne de sous-traitance. Par ailleurs, le contrat doit être régi par le droit de l'État membre dans lequel l'exportateur de données est établi. En outre, l'exportateur demeure responsable par rapport à la personne ayant subi des préjudices du fait d'un manquement aux obligations de sécurité tant de la part de l'importateur que de tout sous traitant ultérieur ;

– Dans le cas où le transfert porte sur des catégories particulières de données (données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques,

---

(1) Cf. décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil.

(2) Cf. documentation de la CNIL : http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/GUIDE-transferts-integral.pdf.

l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle) la personne concernée devra être informée avant le transfert ou dès que possible après le transfert que ses données pourraient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat au sens de la directive 95/46/CE ;

– La personne concernée par le transfert de données peut faire appliquer les clauses types à l'importateur si l'exportateur n'existe plus de droit, et aux sous traitants, si l'importateur n'est, à son tour, plus identifiable. L'action en réparation est ainsi ouverte à tous les niveaux de la chaîne. Elle est d'autre part facilitée par le fait que les clauses doivent prévoir que la personne peut être représentée par une association ;

– Les parties conviennent qu'au terme des services de traitement des données, l'importateur et le sous-traitant ultérieur restitueront à l'exportateur de données, et à la convenance de celui-ci, l'ensemble des données à caractère personnel transférées ainsi que les copies, ou détruiront l'ensemble de ces données et en apporteront la preuve à l'exportateur, à moins que la législation imposée à l'importateur ne l'empêche de restituer ou de détruire la totalité ou une partie des données à caractère personnel transférées. Dans ce cas, l'importateur garantit qu'il assurera la confidentialité des données à caractère personnel transférées et qu'il ne les traitera plus activement.

Si cet encadrement européen resserre de façon conséquente le cadre réglementaire antérieur, il ne dissipe cependant pas toutes les craintes. En cas de disparition des entités juridiques parties aux contrats de sous-traitance des données, les personnes concernées, même réunies au sein d'associations, auront certainement les plus grandes difficultés à faire valoir leurs droits. Les garanties relatives à la remise des données ou à leur destruction ne jouent, en outre, que si l'exportateur ou l'importateur existent en tant qu'entités ; on peut s'interroger sur leur sort lorsqu'elles demeureront sous la seule responsabilité d'un sous-traitant.

La proposition consistant à interdire la sous-traitance des données personnelles et à restreindre les contrats d'externalisation à la seule entité importatrice, sans la possibilité pour cette dernière de se tourner vers un prestataire, demanderait certainement à être évaluée [(1)]. Une disposition plus protectrice, interdisant l'externalisation des données sensibles en dehors de l'Union européenne a fait l'objet de l'orientation n° 27 du présent rapport.

En tout état de cause, ce phénomène étant nouveau et de grande ampleur, une meilleure évaluation de ses conséquences paraît nécessaire.

(1) Avis 3/2009, du 5 mars 2009, concernant le projet de décision de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants de données établis dans des pays tiers en vertu de la directive 95/46/CE.

Orientation n° 34 : mieux évaluer l'importance et les conséquences des transferts de données personnelles dans le cadre du *cloud computing*

Établir un bilan d'évaluation des transferts de données personnelles effectués dans le cadre de l'externalisation des traitements informatiques en dehors de l'Union européenne. Ce bilan aurait pour but de mieux appréhender l'ampleur de ce phénomène, en particulier celui des sous-traitances en cascades, et d'évaluer l'effectivité des différents dispositifs légaux en jeu au regard de la nécessité de préserver les droits des personnes concernées.

*
* *

Cet environnement de communication où aucune garantie absolue de sécurité ne peut être apportée fragilise évidemment les utilisateurs les moins avertis. Les enfants sont les premiers à être mis en danger ; nés avec Internet, les outils numériques influent sur leur mode de vie et déterminent de plus en plus leur culture ; c'est pour eux que la question d'un usage d'Internet respectueux des droits fondamentaux de la personne se pose avec le plus d'acuité.

TROISIÈME PARTIE : LES DROITS DES MINEURS DANS L'UNIVERS NUMÉRIQUE

La nécessité d'une protection accrue des mineurs dans l'univers numérique est sans doute l'une des questions les plus consensuelles comme en témoigne la déclaration finale du G8 de Deauville de mai 2011 : « *Nous nous emploierons (...) à bâtir un environnement dans lequel les enfants pourront utiliser l'Internet sans risque, en améliorant la formation des enfants à l'utilisation de l'Internet, notamment en termes de sensibilisation aux risques, et en promouvant des mesures adéquates de contrôle parental compatibles avec la liberté d'expression.* »

Aussi consensuelle soit-elle, la protection des mineurs dans l'univers numérique est particulièrement difficile à assurer. Si la France a déjà mis en place d'importantes mesures en direction des enfants et des adolescents, ces dernières apparaissent aujourd'hui insuffisantes ou inefficaces au regard des enjeux. Consciente des limites et des difficultés liées à une régulation beaucoup plus poussée de l'Internet, la mission est convaincue que faire du mineur un citoyen bien éduqué, conscient des risques qu'il encourt et des opportunités qui lui sont offertes par le numérique est la meilleure des protections. Cet objectif impose un vaste effort impliquant l'Éducation nationale, les parents, les médias ainsi que l'ensemble des acteurs concernés à travers la co-régulation.

I. LE NUMÉRIQUE : NOUVELLES OPPORTUNITÉS ET NOUVEAUX RISQUES POUR LES ENFANTS ET LES ADOLESCENTS.

A. UNE GÉNÉRATION NUMÉRIQUE

Internet a pris une importance considérable dans la vie des enfants et adolescents et ce, en moins de dix ans, voire moins de trois ans pour les réseaux sociaux : les blogs (sur 10 millions de blogs en France, 80 % proviennent d'adolescents), les chats, les réseaux sociaux, les jeux en ligne, la recherche d'information en ligne, la diffusion et le visionnage de vidéos sur les sites de partage, autant de nouvelles pratiques qui s'ajoutent à une consommation de contenus audiovisuels de plus en plus délinéarisée, qu'il s'agisse de vidéo à la demande ou de télévision de rattrapage.

Financée par le programme *Safer Internet* de la Commission européenne, une enquête sociologique a été réalisée par le réseau scientifique européen *EU Kids Online*, avec la coordination de la *London School of Economics*. Des équipes de chercheurs de 25 pays y ont contribué, dont le CNRS pour la France. Basée sur un échantillon de 25 140 internautes de 9 à 16 ans interrogés, et de leurs parents, cette enquête a été réalisée au cours du printemps et de l'été 2010.

Concernant les usages d'Internet, les statistiques de cette enquête à grande échelle montrent avant tout qu'Internet fait partie intégrante du quotidien des

enfants européens : 93 % des jeunes de 9 à 16 ans se connectent au moins une fois par semaine et 60 % tous les jours ou presque.

L'âge de la première connexion est précoce et tend encore à baisser dans l'ensemble des pays. D'après un sondage IPSOS réalisé en avril 2009 à la demande de l'association e-Enfance, 44 % des 6-8 surfent déjà régulièrement sur Internet. L'enquête sociologique précitée révèle qu'un tiers des internautes européens de 9-10 ans se connectent tous les jours, comme 80 % des 15-16 ans. Utilisé surtout à la maison (87 %) et à l'école (63 %), Internet est également accessible aux enfants dans leur chambre à coucher (49 %) et par l'intermédiaire d'un terminal portable (33 %).

Dans leur grande majorité les 9-16 ans utilisent Internet pour leur travail scolaire (85 %), pour jouer (83 %), regarder des clips vidéo (76 %) et pour la messagerie instantanée (62 %).

Près de 60 % d'entre eux ont un profil sur un réseau social : 26 % des 9-10 ans, 49 % des 11-12 ans, 73 % des 13-14 ans et 82 % des 15-16 ans. En outre, 26 % des jeunes Européens ont un profil public, c'est-à-dire accessible à tout le monde.

B. DES OPPORTUNITÉS NOUVELLES

Ces nouveaux usages apportent aux nouvelles générations des opportunités nouvelles d'information, de loisirs, de création, de communication, d'ouverture extrêmement positives soulignées par la mission dans la première partie du présent rapport.

Si ce sont en général des risques qui sont mis en avant, de nombreux psychiatres et psychologues insistent sur le rôle des technologies numériques comme outil de socialisation douce particulièrement adapté à l'adolescence et vecteur non pas d'isolement mais de liens communautaires.

De nombreuses études scientifiques, menées en France et à l'étranger ont montré les apports du numérique dans l'éducation, à tous les niveaux, école, collège et lycée.

Le développement des usages du numérique dans les pratiques pédagogiques représenterait une véritable opportunité d'amélioration des résultats des élèves, les technologies de l'information et de la communication pour l'éducation (TICE) constituant en particulier des outils d'individualisation de la pédagogie, à destination des enseignants, des élèves, des parents, et plus largement de l'ensemble de la communauté éducative.

Dans les écoles, le numérique permet déjà des avancées pédagogiques inimaginables il y a seulement dix ans. À Élancourt, dans les Yvelines, certaines classes de primaire suivent des cours d'anglais par visioconférence en direct de Grande-Bretagne. L'arrière-pays limougeaud a mis en place un réseau d'éducation

à distance destiné aux élèves habitant en pleine campagne. Dans les Landes, l'école d'Othevielle concocte chaque semaine un « JT des bonnes nouvelles », podcast que toutes les classes de France s'arrachent… Et ce ne sont là que quelques exemples parmi des centaines d'autres.

Le rapport de la mission parlementaire de M. Jean-Michel Fourgous sur la modernisation de l'école par le numérique de février 2010 [(1)] souligne les nombreux effets positifs des TICE sur l'apprentissage des élèves : possibilité d'interactivité, de dédramatisation de l'erreur aboutissant à une augmentation de la motivation ; augmentation de l'envie d'apprendre ; plus grande concentration ; persévérance dans les efforts effectués ; augmentation de la confiance en soi, de la participation en cours, de la collaboration entre élèves ; compréhension plus importante et plus rapide ; meilleure mémorisation ; amélioration des résultats scolaires.

Quant au rapport de l'OCDE sur le dépouillement des tests PISA réalisés en 2006, il met en évidence une corrélation entre les moindres résultats scolaires et l'absence d'ordinateur et d'Internet à domicile, ou plus précisément entre la performance scolaire et la fréquence d'utilisation de l'informatique au domicile (plutôt qu'à l'école). De tels résultats semblent conforter la volonté de mettre des ordinateurs à disposition des plus jeunes, en particulier ceux issus de milieux défavorisés.

C. DE NOUVELLES MENACES

Parallèlement il est vrai que les technologies numériques amplifient des problématiques déjà présentes pour les médias traditionnels : l'exposition aux contenus choquants, pornographiques, de très grande violence, l'impact sur la socialisation et la concentration, notamment en milieu scolaire, les phénomènes de pratiques excessives et d'addiction, la profusion d'informations de toute sorte qui peut être dangereuse si elle ne s'accompagne pas de la capacité de distanciation et de l'esprit critique…, prennent une dimension accrue. À cela s'ajoutent des problématiques nouvelles, résultant de la divulgation massive de données à caractère personnel et de leur possible utilisation par des tiers, ou encore au respect de la législation, concernant notamment les droits d'auteur et la vie privée. Enfin, le développement des usages du numérique auprès des jeunes s'accompagne d'une indépendance croissante des enfants vis-à-vis des parents dans leur consommation de médias : Internet est un terrain plus difficile à restreindre et beaucoup de parents se sentent dépassés.

Concernant les risques liés à l'usage d'Internet, l'enquête précitée, financée par le programme *Safer Internet,* distingue différentes catégories : la pornographie, le harcèlement, la réception de message à caractère sexuel, les

(1) Réussir l'école numérique, *rapport de la mission parlementaire de Jean-Michel Fourgous, député des Yvelines, sur la modernisation de l'école par le numérique.*

contacts avec des inconnus, la lecture de contenus dangereux et le détournement de données personnelles.

Plus de 40 % des internautes âgés de 9 à 16 ans ont été exposés à au moins un de ces risques et le pourcentage augmente avec l'âge : 14 % des 9-10 ans, 33 % des 11-12 ans, 49 % des 13-14 ans et 63 % des 15-16 ans. Le risque le plus répandu est la communication en ligne avec des personnes inconnues.

Une enquête menée par l'association e-Enfance sur 2 670 adolescents de 13 à 18 ans sondés *via Facebook* en mai 2009, montre que 48 % des sondés ont déjà reçu une proposition de rendez-vous avec un inconnu et 20 % déclarent l'avoir acceptée (30 % pour les garçons de 13-14 ans) ; 29 % ont fait l'objet de propositions sexuelles (43 % des filles de 13-14 ans) et 53 % ont été confrontés à des images de pornographie ou de violence. 76 % des enfants gardent leurs mésaventures pour eux, révèle la deuxième partie de l'étude, un sondage IPSOS mené auprès des 9-17 ans. Il indique aussi que plus des deux tiers avouent ne pas respecter les consignes parentales de prudence.

L'enquête commandée par le programme *Safer Internet* révèle pourtant que la plupart des enfants disent surfer sans que cela n'engendre pour eux des problèmes ou des inquiétudes quelconques. Seuls 12 % des internautes âgés de 9 à 16 ans (9 % des 9-10 ans) disent avoir été ennuyés ou tracassés par quelque chose sur Internet. Les risques encourus ne sont pas forcément vécus par les enfants comme des expériences traumatisantes. Si 14 % des 9-16 ans ont vu des images pornographiques ou à caractère sexuel sur Internet, ou encore si 9 % ont eu rendez-vous avec une personne qui les avait rencontrés sur Internet, peu d'entre eux considèrent qu'il s'agit là d'expériences difficiles, soit respectivement 33 % et 1 % pour chacun des deux cas cités. Le harcèlement en ligne par des messages blessants ou agressifs, concerne 6 % des enfants, c'est le risque qu'ils ressentent comme le plus douloureux.

Les mineurs sont particulièrement concernés par la problématique de la vie privée et des données personnelles dans la mesure où ils exposent leur vie intime sur les réseaux sociaux sans être toujours conscients des conséquences que cela peut entraîner et sans que l'on puisse s'en remettre à leur responsabilité. Pour les jeunes, *Facebook* est devenu un enjeu de sociabilité dont les bénéfices seraient plus importants que les risques encourus. Les adolescents auraient une conception différente de leur vie privée de ceux qui n'ont pas grandi avec Internet.

Pour M. Jean-Emmanuel Ray, professeur de droit du travail à l'Université Paris I-Sorbonne, auditionné par la mission le 2 mars 2011, le problème le plus inquiétant concerne l'usage qui sera fait dans quelques années des informations qui se seront accumulées sur les enfants d'aujourd'hui. En seulement quatre années, *Facebook* a révolutionné les écoles et les collèges. Qu'en sera-t-il dans quinze ans ? Toutes les informations que les jeunes auront diffusées resteront accessibles et seront à disposition, par exemple, des recruteurs.

La construction du rapport des enfants à la citoyenneté et au respect de la loi est un autre enjeu très important dans l'univers numérique. L'apparente anonymisation de l'accès à Internet peut véhiculer des illusions, comme la virtualité des actes, un certain sentiment d'impunité, que ce soit concernant le respect de la dignité des personnes, le respect de la vie privée ou celui des droits d'auteurs.

Comme l'a rappelé M. Jean-Emmanuel Ray, sur Internet, les personnes, notamment les plus jeunes, ne savent pas qu'elles agissent mal, à la différence des délinquants dans la vie réelle. *Facebook* appartient au monde du virtuel ; en conséquence, tout paraissant virtuel, y sont tenus des propos qui ne l'auraient jamais été dans le réel.

Or il est important que les enfants et les adolescents comprennent qu'il n'y a pas d'impunité sur Internet, et qu'il existe un cadre légal qui doit être respecté, que les injures, la diffamation, les atteintes à la vie privée et à la confidentialité constituent des fautes pénales.

M. Jean-Emmanuel Ray a souligné l'ampleur d'un autre phénomène résultant du développement des technologies numériques, dont l'impact sur les mineurs est moins évident. Inexorablement, le temps de la vie privée serait selon lui grignoté par celui du travail. Les pédopsychiatres s'en inquiètent car un parent présent doit être un parent disponible. Mieux vaut encore que le parent reste travailler au bureau que d'être présent sans être disponible pour son entourage. La dérive est extrêmement dangereuse : les enfants ne comprennent pas la situation et les salariés sont en butte aux plaintes de leur famille. Il serait donc hautement souhaitable que les salariés trouvent un équilibre et fassent comprendre la distinction entre le fait d'être joignable et celui d'être « dérangeable ». En Allemagne, ont été signés des accords collectifs opposables qui interdisent, sauf exceptions, de joindre les employés après 17 heures le vendredi. Trois entreprises françaises parlent déjà dans leurs accords collectifs – et dans leur propre intérêt – de droit à la déconnexion.

Orientation n° 35 : Promouvoir le droit à la déconnexion

Le droit pour les salariés de ne pas être connecté constamment à leur outil de travail numérique doit être promu au sein des entreprises.

D. DE NOUVEAUX BESOINS

À l'heure où les outils numériques sont omniprésents dans la société, dans les relations sociales et dans le monde de l'entreprise, l'acquisition des compétences numériques est déterminante pour une future insertion sociale et professionnelle réussie. Donner toutes les cartes au futur citoyen pour s'intégrer dans la société du numérique et de l'information est une mission essentielle de l'éducation : la multiplication des échanges et des sources d'information implique

une éducation à l'usage responsable de l'Internet et des technologies de l'information et de la communication.

Le développement du numérique impose de nouveaux apprentissages. Apprendre qu'un blog et un réseau social peuvent être un espace public, que les mots et les images qui y sont diffusés peuvent avoir des conséquences qui ne sont pas virtuelles, apprendre comment retirer une référence, une photo, apprendre qu'il n'y a pas d'impunité pour les insultes, la diffamation sont autant de compétences nouvelles que les enfants doivent acquérir pour pouvoir évoluer sereinement sur Internet.

Le développement des usages d'Internet nécessite tout d'abord une éducation à la fiabilité et à la hiérarchisation des sources, des données, des informations et une compréhension, ou à tout le moins, une analyse critique, des principes régissant le référencement par les moteurs de recherche.

Il y a là un enjeu d'égalité dans l'accès à la connaissance, comme l'a souligné M. Dominique Wolton, lors de son audition du 30 juin 2010, en insistant sur le fait que disposer d'une information sans avoir les outils pour la comprendre conduit toujours à l'échec. C'est pourquoi cette éducation est absolument primordiale pour la formation de citoyens capables d'exercer leur libre arbitre et de participer activement à la démocratie. De plus en plus, les enseignants demandent à leurs élèves de faire des recherches sur Internet ; il est nécessaire de leur en fournir les règles. M. Dominique Wolton a rappelé à la mission que d'après une enquête IPSOS/e-Enfance, 92 % des parents ne pensent pas à dire à leurs enfants que tout n'est pas vrai sur Internet. Cette dimension de l'éducation aux médias doit donc être portée par l'école républicaine et par le service public de l'audiovisuel.

M. Bernard Benhamou, délégué aux usages de l'Internet auprès du ministère de l'Enseignement supérieur et de la recherche et du secrétariat d'État chargé de la prospective et du développement de l'économie numérique, a également souligné que, faute d'éducation du citoyen au numérique, il pourrait se produire, outre la fracture numérique, une fracture d'usage entre ceux qui maîtriseraient les nouvelles technologies et en retireraient un bénéfice social, culturel ou professionnel et ceux qui n'en maîtriseraient que l'aspect ludique de consommation.

La protection des données personnelles et la gestion de la vie privée à l'ère numérique exigent une connaissance approfondie des risques, des droits et des devoirs en la matière.

La place prise par les réseaux sociaux, l'extension accélérée du nombre des fichiers nominatifs institutionnels ou commerciaux, le développement des techniques de « traçage » (puces *RFID*, téléphones portables, GPS), la perspective d'un « Internet des objets » imposent une vigilance accrue face à l'ampleur des données personnelles qui sont collectées et l'usage qui peut en être fait.

À cet égard, Mme Véronique Fima-Fromager, directrice de Action innocence, s'est montrée très critique sur la notion de droit à l'oubli. Cette dernière laisse penser qu'il existerait un droit à l'oubli numérique, ce qu'elle récuse et que personne n'est en mesure d'affirmer. Laisser croire aux adolescents qu'il existe un droit à l'oubli leur donne l'illusion que ce qu'ils font sur Internet ne pourra pas leur porter préjudice demain alors qu'il conviendrait au contraire d'accroître leur vigilance et de les responsabiliser.

Ajoutons que beaucoup de questions sont posées et des études sont à mener concernant les effets de ces nouvelles modalités d'apprentissage, d'information et de travail sur le fonctionnement même de l'intelligence et sur les procédures cognitives (mode de perception et de représentation, raisonnement, mémoire…).

Il semblerait que les enfants et adolescents ne soient plus ce qu'ils étaient. « *Les technologies de l'information et de la communication appliquées à l'éducation changent nos manières de penser et d'agir, d'où un impact fort sur l'école, en termes de rapport au savoir, à l'autorité, à l'évaluation* », reconnaît M. Richard-Emmanuel Eastes, spécialiste des sciences cognitives appliquées à l'éducation. « *L'école d'hier nous a habitués à des réponses claires et uniques. À présent, d'innombrables interrogations émergent de l'explosion des blogs et des forums de discussion. Et les réponses ne sont plus uniques, en vertu de la mutualisation des connaissances de milliers d'internautes.* » (1)

Les « *digital natives* », indigènes de l'univers numérique dans lequel ils sont nés et avec lequel ils ont grandi, ont des attentes et des compétences différentes. Selon M. Marc Prensky, spécialiste américain des TICE et inventeur de l'expression, les« *digital natives* » sont de plus en plus multitâches, autrement dit, ils sont capables de faire leurs devoirs tout en chattant sur MSN, entre deux envois de SMS, l'iPod sur les oreilles. Que cette évolution soit positive ou négative, il convient d'en tenir compte car, selon M. Marc Prensky, « *les élèves d'aujourd'hui ne sont plus ceux que notre système éducatif était censé former* ».

Selon M. Daniel Andler, philosophe, spécialiste des sciences cognitives, fondateur de COMPAS, un « *think tank* » de l'École normale supérieure réunissant chercheurs et professeurs de toutes les disciplines ainsi que quelques industriels pour réfléchir aux pédagogies du futur, la génération numérique s'éloigne de plus en plus d'un apprentissage dogmatique, combinant mémorisation pure et logique d'entraînement/récompense. En revanche, « *les jeunes adoptent volontiers des processus d'apprentissage fondés sur la déconstruction/reconstruction des savoirs, sur l'interactivité des méthodes et des points de vue… un peu sur le modèle des jeux vidéo, qui permettent de passer au niveau 1, puis au niveau 2, etc. en essayant différentes clés, quitte à aller dénicher la solution sur des sites spécialisés. Ils ont intégré le fait qu'on peut apprendre en se trompant, qu'on peut recycler à son profit les expériences d'autrui.* » (2) Il

(1) RSLN, mars 2008, « Bienvenue à l'école du futur ».
(2) Ibid.

s'ensuit que ce n'est plus le savoir lui-même qui est essentiel, mais bien l'habileté à trier et à décoder l'information proposée en ligne.

Ces mutations doivent inévitablement pousser l'école et la pédagogie à se transformer. Pour que l'école de demain soit une réussite, les spécialistes s'accordent à penser qu'il faut une réforme holistique c'est-à-dire globale – qui implique le rapport entre le professeur et l'élève, la pédagogie, les technologies, l'organisation du temps, de l'espace, etc.

II. UNE PRISE EN COMPTE DES ENJEUX DU NUMÉRIQUE POUR LA JEUNESSE RÉELLE MAIS INSUFFISANTE

S'agissant de l'arsenal législatif existant, lors de la table ronde sur la protection de l'enfance à l'ère numérique organisée par la mission le 9 novembre 2010, Mme Véronique Fima-Fromager, directrice d'Action innocence, a considéré que la France faisait partie des rares pays européens où l'ensemble des sujets ont fait l'objet de mesures législatives mais s'est déclarée plus sceptique sur leur application, tout en reconnaissant que tout ne saurait toutefois passer par la loi.

A. LE RÔLE DE L'ÉDUCATION NATIONALE

L'éducation est confrontée à trois défis majeurs. Elle doit apprendre à l'enfant à se servir des technologies numériques et à en connaître les écueils. Elle doit tirer parti de toutes leurs potentialités, y compris dans l'évolution des méthodes pédagogiques et la lutte contre l'échec scolaire, et répondre ainsi aux attentes d'une nouvelle génération. Elle doit enfin accompagner la communauté éducative dans son appropriation des TICE.

1. Le numérique à l'école : situation actuelle

La Ligue de l'enseignement, dans sa contribution écrite aux réflexions de la mission, a estimé que des avancées estimables, malgré les lenteurs dues à des obstacles techniques, pédagogiques et organisationnels, avaient été accomplies sur l'appropriation des technologies numériques en classe, et notamment sur la réflexion citoyenne par rapport à ces usages.

« *Reste que ce qui émerge des différents coups de sonde sur ce qui se passe dans les établissements scolaires, c'est le sentiment que la culture numérique et les retombées qu'elle devrait avoir sur l'organisation et les contenus des apprentissages n'y sont pas assez sérieusement prises en compte. Un même constat avait pu être fait naguère pour la culture de l'image, mais l'enjeu était, somme toute, moins essentiel.* »

Il semblerait que l'on essaie très généralement de faire rentrer des modèles anciens dans des formes nouvelles.

Le plus souvent le numérique n'est utilisé que comme un nouveau support – souvent plus commode, certes – pour véhiculer le cours magistral ou pour décalquer l'organisation pédagogique traditionnelle. Ceci reste vrai pour les usages du tableau blanc interactif, bien qu'il soit présenté comme une révolution pédagogique, pour les manuels numériques et pour le cahier de texte numérique, même si ce dernier remporte un certain succès auprès des parents pour des raisons souvent ambiguës (en tant qu'outil de surveillance des enseignants par les parents et par l'inspection). Cela vaut également pour les usages qui sont faits le plus souvent des ENT (environnements numériques de travail) alors que ceux-ci devaient ouvrir des perspectives très novatrices dans l'organisation de la scolarité.

Au lieu d'être considéré comme un nouveau support pour des exercices traditionnels, l'ordinateur devrait en effet conduire à changer les contenus et les méthodes de l'enseignement. L'existence des technologies numériques entraîne en effet une modification de la nature même des disciplines enseignées : recherche documentaire, création artistique et littéraire, cartographie en géographie, simulation dans de nombreuses disciplines, expérimentation assistée par ordinateur en sciences physiques et chimiques et en sciences de la vie et de la terre, etc. Elle entraîne aussi la possibilité de méthodes de travail différentes, pour la recherche documentaire, le travail coopératif, les modes d'évaluation. Trop souvent, les usages de l'ordinateur restent cependant dans une conception purement transmissive du savoir, et ne font que rénover, de façon plus « attrayante » et plus « ludique » les méthodes déjà en usage.

Deux raisons principales peuvent expliquer ces « retards à l'allumage » :

– premièrement, les élèves n'ont en général pas accès directement et personnellement à une machine : la « salle informatique », qui est toujours présente dans certaines écoles, ou les équipements mobiles ne permettent que des « exercices » ponctuels. Pour arriver à une utilisation régulière, chaque élève devrait disposer d'un outil individuel et mobile pouvant se connecter au réseau de l'école ou de l'établissement. Sur ce point, l'obstacle est évidemment financier. L'État espère beaucoup pouvoir mobiliser les collectivités territoriales pour arriver à ce type d'équipement, mais les contraintes budgétaires et organisationnelles qui pèsent sur elles pourraient bien contrarier cet espoir. N'oublions pas non plus que l'aménagement complet du territoire n'est pas réalisé et qu'il demeure des zones où l'on n'a, en tout état de cause, pas accès au haut débit ;

– deuxièmement, les programmes scolaires, les méthodes de travail des élèves et les formes d'évaluation ne sont pas conçus pour engager ces évolutions.

S'agissant des contenus de la formation des élèves, lors de la table ronde du 9 novembre 2010, Mme Deborah Elalouf, présidente-directrice générale de la société Tralalere, en charge de l'animation du programme « Internet sans crainte », a rappelé, s'agissant du B2i, que la France fait partie des rares pays à prévoir, dans le cadre du cursus scolaire, un passage obligatoire permettant d'aborder les usages de l'Internet.

Le décret n° 2006-830 du 11 juillet 2006 relatif au socle commun de connaissances et de compétences, qui détermine ce que « *nul n'est censé ignorer en fin de scolarité obligatoire, sous peine de se trouver marginalisé ou handicapé* », fait figurer explicitement l'éducation aux médias parmi les objectifs fondamentaux officiellement assignés au système éducatif, notamment en ce qui concerne les piliers 4 et 6 du socle (soit « la maîtrise des techniques usuelles de l'information et de la communication » d'une part et « les compétences sociales et civiques » d'autre part). Chaque élève doit apprendre à faire un usage responsable des technologies de l'information et de la communication (TIC).

L'acquisition du Brevet informatique et Internet (B2i) est même nécessaire à l'obtention, en fin de troisième, du Diplôme national du brevet.

En février 2001, le ministère de l'Éducation nationale a déposé la marque « B2i ». L'objectif de ce brevet est d'attester le niveau acquis par les élèves dans la maîtrise des outils multimédias et de l'Internet.

Tous les écoliers, collégiens et apprentis des centres de formation des apprentis gérés par les établissements publics locaux d'enseignements (EPLE) sont concernés par cette attestation.

Les compétences évaluées dans le cadre du B2i sont les suivantes : s'approprier un environnement informatique de travail ; adopter une attitude responsable ; créer, produire, traiter, exploiter des données ; s'informer, se documenter ; communiquer et échanger.

Le B2i, qui offre un bon équilibre entre le développement des compétences liées aux usages techniques et aux « bons usages » (ou usages citoyens, développant la créativité, l'esprit critique, la réflexion sur les libertés publiques et privées) de l'ordinateur a pu se généraliser au collège, du fait qu'il est nécessaire pour l'obtention du Brevet national des collèges.

Il est cependant peu connu du public et les enseignants semblent peu concernés par la réflexion sur ses contenus. À l'école primaire, si le B2i est intégré aux programmes depuis 2002, toutes les écoles ne le mettent pas encore en œuvre et en juin 2008, un peu moins de 30 % des élèves sortants de CM2 ont obtenu le B2i [(1)].

Quelques remarques peuvent être faites à ce sujet :

– le mode d'évaluation en cours de formation et par compétences pour le B2i, qui marquait une rupture avec les modes d'évaluation traditionnels, retombe progressivement vers des exercices classiques effectués après un « cours de B2i » ;

(1) Source : enquête ETIC 2008-2009.

– plus du tiers des enseignants déclarent qu'ils n'ont pas les compétences pour contribuer aux acquisitions des élèves demandées dans le cadre du B2i. Il semble pourtant – et c'est une bonne chose – que cette formation aux compétences du B2i et la validation de ces compétences ne soient plus, comme elle le fut trop longtemps, le monopole des professeurs de technologie ;

– le socle commun des compétences n'est pas vraiment mis en application dans les établissements.

L'éducation aux médias est par ailleurs censée irriguer l'ensemble des programmes.

À l'école primaire, au terme du cycle 3 (CE2-CM2), les programmes précisent que les élèves doivent ainsi être en mesure de « *faire preuve d'esprit critique face à l'information et à son traitement* ».

Au collège, l'éducation aux médias figure également dans les programmes, notamment dans le cadre de l'éducation civique.

Au lycée, les médias doivent être présents dans les différents programmes (en éducation civique, juridique et sociale (ECJS), en cours de français, d'histoire, de sciences de la vie et de la Terre).

En réalité, l'éducation aux médias demeure peu présente en tant que telle dans les politiques éducatives, comme l'a rappelé un rapport d'août 2007 sur l'éducation aux médias de l'inspection générale de l'éducation nationale (IGEN) et de l'inspection générale de l'administration, de l'éducation nationale et de la Recherche alors même que les programmes recommandent assez largement d'introduire les médias dans les pratiques de classe, comme supports pédagogiques, comme outils d'apprentissage ou comme objets d'étude. Les instructions passent souvent inaperçues et restent lettre morte. Les obstacles structurels et les résistances culturelles sont en effet multiples : les objectifs sont mal définis, le champ de l'action est vaste et confus, la formation des enseignants est insuffisante, les horaires d'enseignement sont rigoureusement contraints.

Selon le rapport de l'IGEN précité, l'éducation aux médias est donc restée, majoritairement, « une affaire de militants », reposant sur des moyens non stabilisés. Il existe encore, manifestement, un fossé important entre le discours affiché et la situation réelle sur le terrain.

Le CLEMI (Centre de liaison de l'Enseignement et des Médias d'Information) participe également à l'éducation aux médias dans les établissements. À travers l'action du CLEMI, la France a été un précurseur en matière d'éducation aux médias. Cet organe est en effet chargé en partenariat avec le ministère de l'Éducation nationale, de l'éducation aux médias dans l'ensemble du système éducatif et a pour objectif d'apprendre aux élèves une pratique citoyenne des médias par le biais notamment de partenariats entre les enseignants et les professionnels de l'information.

Auditionnée le 3 novembre 2010 par la mission, Mme France Renucci, directrice CLEMI, a expliqué que celui-ci formait, au sein du ministère de l'Éducation nationale, une petite structure organisée en réseau qui comprenait vingt enseignants travaillant au niveau national et des coordonnateurs nommés par les recteurs. Ces derniers ont pour fonction de constituer des équipes d'enseignants chargés d'actions de formation qui s'adressent à tous les niveaux scolaires et à toutes les disciplines. Tous les enseignants, quels que soient leur niveau et leur discipline peuvent venir se former au CLEMI qui travaille en réseau avec un coordinateur dans chaque académie et forme ainsi depuis vingt-cinq ans environ 30 000 enseignants chaque année.

Le CLEMI procède, par ailleurs, à une analyse systématique des programmes scolaires pour y repérer la part qui y est réservée à l'enseignement des médias.

L'action phare du CLEMI est depuis vingt ans la semaine de la presse et des médias à l'école. Elle est conduite en partenariat avec des journalistes et des médias locaux et nationaux et permet à plus de quatre millions d'élèves mobilisés dans 15 000 établissements de mieux connaître les techniques et le langage des médias.

Le travail du CLEMI est cependant loin de concerner la majorité des établissements. En outre, le caractère événementiel de la semaine de la presse et des médias agit comme une piqûre de rappel là où un véritable traitement de fond est nécessaire.

2. La question de la formation des enseignants

D'après les textes, tous les enseignants réussissant les concours de recrutement devraient être titulaires du Certificat informatique et Internet (C2i) niveau 2 enseignants. Tous, en effet, devraient être capables de contribuer aux formations B2i école, B2i collège ou B2i lycée. Par ailleurs le C2i niveau 1 est exigible dans tous les cursus universitaires. Les contenus de ces formations font tous une part satisfaisante aux usages raisonnés du numérique et à la problématique Informatique et Libertés. Comme pour le B2i des élèves, c'est plutôt leur mise en œuvre qui semble poser quelques problèmes.

Selon Mme Émilie Peinchaud, chargée de communication de « Internet sans crainte », entendue lors de la table ronde du 9 novembre 2010, concrètement, un enseignant ayant un certain bagage informatique sera en mesure de proposer des activités réflexives et intéressantes à ses élèves, ce qui ne sera pas le cas s'il n'a aucune expérience des ordinateurs. Cette question est laissée à la responsabilité de chaque enseignant et aboutit à des résultats aléatoires et très variables sur le terrain.

Concernant le « Certificat informatique et Internet niveau 2 enseignants » (C2i2e), la Ligue de l'enseignement observe qu'avec la disparition des IUFM, il

existe une grande inconnue actuellement sur le point de savoir qui assurera la formation requise ; il n'est pas certain, si les UFR en sont chargées, qu'elles disposent en leur sein des compétences correspondant aux aspects professionnels de cette formation. De plus, lors de la création du C2i niveau 2 enseignant, il était envisagé que l'exigence de ce certificat ne s'applique pas seulement aux enseignants nouvellement recrutés, mais concerne progressivement tous les enseignants au travers de la formation continue. Il ne semble pas que cette intention initiale ait été mise en œuvre.

Selon Mme France Renucci, directrice du CLEMI, des efforts restent à faire dans la préparation des étudiants qui se destinent à l'enseignement. Au-delà du C2i, il conviendrait de rendre plus systématique l'enseignement aux médias pour que celui-ci devienne effectif dans chaque discipline.

Il serait opportun d'instituer une semaine consacrée à l'éducation aux nouveaux médias dans le cadre de la formation initiale des enseignants ainsi que lors de la formation continue.

Dans le cadre du plan de développement des usages du numérique à l'école, l'accompagnement des enseignants et leur formation sont considérés comme un facteur clé de succès. Dans chaque établissement, sur la base du volontariat, un professeur responsable du numérique pédagogique sera ainsi désigné, afin de conseiller le chef d'établissement dans la définition et la mise en œuvre de la politique numérique et dans l'identification des besoins de formation de ses collègues et leur réalisation. Ce plan de formation au plus près de l'établissement sera complémentaire des formations académiques aux usages du numérique et aux formations en ligne.

3. Faire de l'éducation civique aux médias un cursus obligatoire, repenser le B2i et accroître la place du numérique à l'École

Mme Deborah Elalouf, présidente de la société Tralalere, en charge de l'animation du programme « Internet sans crainte », a rappelé, lors de la table ronde du 9 novembre 2010 que l'une des priorités d'Internet sans crainte était l'éducation critique des jeunes et des médiateurs éducatifs ainsi que des parents, sur la base d'une posture réflexive et d'un équilibre à trouver entre protection d'une part, et promotion des usages positifs d'autre part.

Mme Sophie Jehel, membre du conseil scientifique du collectif interassociation « Enfance et Médias » a appelé de ses vœux une disposition législative comportant une obligation d'intégrer l'éducation aux médias dans un cursus.

Le rapport de la Commission famille, éducation aux médias, composée de représentants des associations et d'institutions publiques, ainsi que de professionnels des médias, remis en juin 2009 à Mme Nadine Morano, alors secrétaire d'État chargée de la famille estimait que l'éducation aux médias devait devenir un véritable cursus obligatoire, à l'école primaire, au collège, au lycée,

avec plusieurs dizaines d'heures d'enseignement. Le rapport soulignait que la maternelle ne devait pas être oubliée avec une découverte des médias et de l'image. L'éducation aux médias serait assurée au niveau du collège et du lycée par les professeurs documentalistes dont le rôle pivot serait réaffirmé et la formation aux nouveaux enjeux d'Internet améliorée.

La loi n° 2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques a complété l'article L. 312-15 du code de l'éducation par un alinéa ainsi rédigé : « *Dans le cadre de l'enseignement d'éducation civique, les élèves sont formés afin de développer une attitude critique et réfléchie vis-à-vis de l'information disponible et d'acquérir un comportement responsable dans l'utilisation des outils interactifs, lors de leur usage des services de communication au public en ligne. Ils sont informés des moyens de maîtriser leur image publique, des dangers de l'exposition de soi et d'autrui, des droits d'opposition, de suppression, d'accès et de rectification prévus par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que des missions de la Commission nationale de l'informatique et des libertés.* »

La mission se félicite de cette initiative de la sénatrice Mme Catherine Morin-Desailly, qui apparaissait déjà dans la proposition de loi déposée par M. Détraigne et Mme Escoffier telle qu'adoptée par le Sénat, et appelle de ses vœux une véritable mise en œuvre de cette disposition qui implique une réflexion sur son articulation avec la dimension « éducation civique » du B2i.

Lors de la table ronde du 9 novembre 2010, Mme Véronique Fima-Fromager, directrice de Action innocence, a estimé que le B2i avait beaucoup vieilli et qu'il devait être adapté au regard de l'évolution des technologies et des usages. Il convient, selon elle, d'y intégrer la dimension sociale, éthique et citoyenne afin de renforcer et d'actualiser le principe de ce brevet qui ne vise originellement qu'à apprendre aux enfants à se servir d'Internet, alors que l'usage d'Internet par les jeunes est, le moins que l'on puisse dire, aujourd'hui extrêmement répandu.

Selon le plan de développement des usages du numérique à l'école, « *pour accompagner les élèves dans leur appropriation de la société numérique, l'éducation nationale doit former les citoyens numériques de demain, en transmettant les valeurs civiques dans la société de l'information. Au-delà de la formation technique, le Brevet informatique et Internet, qui valide les compétences numériques acquises par les élèves, accordera dès la rentrée 2011 plus d'importance à l'apprentissage de l'usage responsable de l'Internet. Les équipes pédagogiques et les élèves pourront s'appuyer dès le début 2011 sur un portail de ressources pédagogiques sur ce thème.* »

Il importe également que soit envisagée une modification des programmes et des méthodes d'enseignement et d'évaluation afin que le numérique devienne partie intégrante de l'enseignement, et non un simple outil.

Pour promouvoir l'utilisation des ressources numériques pédagogiques innovantes, le plan de développement des usages du numérique à l'école publié le 25 novembre 2010 prévoit que le ministère mettra en place un portail de référencement des ressources pédagogiques, de l'édition publique et privée. Ce portail permettra aux équipes pédagogiques de découvrir les ressources les plus pertinentes pour ses besoins. Les établissements et écoles retenus dans le cadre de l'appel à projets seront dotés d'un « chèque ressources numériques », leur permettant d'acquérir des ressources numériques pédagogiques, complément indispensable de l'équipement et des services numériques.

S'agissant des aspects matériels, il convient de faire en sorte que les élèves puissent avoir un accès facile et constant (à l'école, à leur domicile) à un outil numérique. Aux termes du plan de développement des usages du numérique à l'école, « *persuadé de l'intérêt d'ouvrir l'École vers l'extérieur, le ministère a enclenché la généralisation du cahier de textes numérique depuis la rentrée 2010. Ce service numérique permet aux enseignants, élèves et parents de suivre la progression pédagogique de sa classe. Plus largement, le ministère, en partenariat avec les collectivités territoriales, réaffirme l'objectif de généraliser les Espaces numériques de travail* (1)*, véritables bouquets de services de la communauté éducative sur l'ensemble du territoire*. » L'équipement en « tableaux numériques » des classes doit également devenir une priorité.

Orientation n° 36 : renforcer l'éducation aux médias et la place du numérique à l'école :

– mettre en place un enseignement spécifique d'éducation au numérique dans le cadre de l'éducation civique, conformément aux dispositions de la loi n° 2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques et réfléchir à son articulation avec le B2i ;

– dans le cadre du B2i, donner plus d'importance à l'apprentissage de l'usage responsable de l'Internet. Développer davantage le B2i à l'école primaire ;

– améliorer la formation des enseignants aux outils et services numériques ;

– permettre à chaque élève de disposer d'un outil individuel et mobile permettant de se connecter au réseau de l'école ou de l'établissement ;

– généraliser les espaces numériques de travail (ENT) ;

– créer de nouveaux supports interactifs et des manuels numériques innovants ;

- lancer une réflexion sur une réforme plus globale des programmes et des méthodes d'enseignement et d'évaluation afin de mettre le numérique au service d'une pédagogie renouvelée.

(1) Ensemble intégré de services numériques, choisi, organisé et mis à disposition de la communauté éducative par l'établissement scolaire.

B. LE RÔLE DES PARENTS

1. Le contrôle parental : le maillon faible

Le rapport des parents à la consommation de médias de leurs enfants change profondément avec le développement du numérique. La consommation de contenus délinéarisée ou mobile, plus individualisée, avec une multiplication des écrans auquel l'enfant peut accéder seul, rend inopérants les dispositifs traditionnels de protection de l'enfance (comme la signalétique par exemple). Le triptyque traditionnel, « choisir avant, regarder avec, parler après », déjà loin d'être appliqué dans les foyers, devient encore plus difficile à mettre en œuvre.

Une étude Trend Micro de mars 2009 montre que la chambre est le premier lieu où les adolescents ont une consommation médiatique sur Internet. Chez les jeunes parents (entre 25 et 34 ans), près d'un enfant sur deux (44,4 %) accède à Internet dans sa chambre [(1)]. Les parents ont donc de grandes difficultés pour cerner l'utilisation qu'ont leurs enfants d'Internet.

Toujours selon la même étude, chez les parents, qui sont 40 % à être bien conscients de l'utilisation régulière de cet outil, seulement 32 % estiment connaître les « contacts » de leurs enfants, proportion qui baisse à mesure que les parents vieillissent. En effet, la majorité des plus de 55 ans (57 %) n'en connaissent que quelques-uns, voire aucun pour 14 %.

D'après un sondage IPSOS d'avril 2009, 43 % des parents reconnaissent ne pas donner systématiquement de règles à leurs enfants sur Internet. Et même lorsque des règles sont données, elles ne sont pas forcément respectées par les enfants : sur cinq règles prudentielles (ne pas se rendre à un rendez-vous d'un inconnu, ne jamais dévoiler des informations intimes, ne pas répondre aux messages des gens qu'on ne connaît pas, vérifier ce qui est écrit car tout n'est pas vrai sur Internet, ne pas passer trop de temps sur Internet), 35 % des enfants (9-17 ans) déclarent respecter toutes les règles, mais 65 % déclarent ne pas respecter au moins une règle.

L'autre enseignement de l'enquête précitée financée par le programme *Safer Internet* de la Commission européenne est la sous-estimation par les parents des risques encourus par leurs enfants : 40 % des parents des 9-16 ans qui ont vu des images sexuelles et 56 % des parents dont les enfants ont reçu des messages agressifs pensent que cela ne leur est pas arrivé. Les parents sont également nombreux à ignorer que leurs enfants ont reçu des messages sexuels (52 %) ou qu'ils ont rencontré une personne connue par Internet (61 %). Pourtant la plupart des parents (70 %) déclarent parler avec leurs enfants de ce qu'ils font sur Internet, plus de la moitié d'entre eux (56 %) leur donnent des conseils sur la façon de communiquer en ligne. Seuls 28 % des parents utilisent des dispositifs

(1) L'étude a été conduite entre le 12 mars et le 19 mars 2009 auprès d'un échantillon représentatif de 505 parents âgés de 16 à +55 ans et de 505 enfants âgés de 12 à 18. Les interviews ont été menées sur Internet.

techniques de contrôle et 24 % regardent tout simplement l'historique de navigation de leurs enfants. La plupart des parents (73 %) pensent qu'il est « *peu probable* » ou « *pas du tout probable* » qu'il arrive quelque chose à leur enfant sur Internet dans les six prochains mois.

En matière de sécurité sur Internet, les enfants prennent des conseils auprès de leurs parents (63 %), de leurs enseignants (58 %) et de leurs amis (44 %). Les adolescents les plus âgés et ceux ayant des origines sociales modestes s'adressent plus souvent aux enseignants qu'à leurs parents. En guise de conclusion, les auteurs de cette étude invitent la Commission européenne à encourager l'éducation des enfants, comme celle des parents et le développement d'outils de contrôle parental.

Au–delà de l'interdiction pure et simple de l'accès à des sites au contenu délictueux voire criminel, l'usage des logiciels de contrôle parental se répand enfin. Ces programmes permettent de filtrer l'accès au Net depuis chaque ordinateur, téléphone ou console de jeu vidéo, en bloquant la consultation des informations choquantes pour les enfants ou les adolescents (sexe, racisme, violence…). Certains logiciels empêchent également que le jeune utilisateur transmette la moindre donnée personnelle (courriel, numéro de téléphone, adresse) et interdisent toute transaction bancaire.

Enfin, pour sécuriser davantage encore la navigation des plus jeunes, il existe des systèmes de « listes blanches » permettant de circonscrire l'accès à une liste prédéfinie de sites, sorte de jardin d'enfant virtuel complètement protégé.

Le filtrage des sites pornographiques est aujourd'hui assuré en moyenne à 80 %, et celui des sites d'argent à 90 %. Pour les sites violents ou racistes, ainsi que les sites incitant à la consommation de drogues, le taux de filtrage se situe dans une fourchette de 50 à 60 %, alors qu'il était aux alentours de 20 à 30 % en 2006.

Les diffuseurs privilégiés des logiciels de contrôle parental sont les FAI. Depuis 2006, ils ont l'obligation de fournir gratuitement à tous leurs abonnés un programme de filtrage. Décidé à faire de la qualité de ces logiciels un critère de choix, le gouvernement publie un classement, qui devrait bientôt être affiché chez les distributeurs. Numéricable arrive en tête (taux de filtrage atteignant 88 % toutes catégories de sites confondues), suivi de Free, Alice, Orange, SFR, Télé 2, Neuf. Darty ferme la marche, avec un taux de filtrage de 75 %.

Les spécialistes sont unanimes sur ce point : les logiciels de contrôle parental sont indispensables. Reste à convaincre les parents de s'en servir.

2. Propositions pour renforcer le contrôle parental

• **Mettre en place une grande campagne d'information et de sensibilisation**

Pour M. Benoît Tabaka, secrétaire général de l'Association des services Internet communautaires (ASIC), auditionné le 29 septembre 2010, s'agissant de la protection des mineurs, un opérateur ne peut pas s'assurer qu'un mineur est effectivement âgé de moins de treize ans. Il faut donc dire aux parents d'installer l'ordinateur dans leur salon et non dans la chambre de l'enfant.

Pour mieux assurer la protection des mineurs, la seule voie à suivre serait celle de la sensibilisation des parents.

Lors de la table ronde du 9 novembre 2010, M. Serge Tisseron, psychologue, spécialiste des rapports aux nouvelles technologies, a estimé qu'il faudrait beaucoup mieux sensibiliser les parents sur le moment où ils peuvent introduire les nouvelles technologies dans la vie de l'enfant. Dans le cadre du travail qu'il accomplit au sein de classes de primaire, M. Serge Tisseron s'est dit effaré de découvrir qu'environ la moitié des enfants du primaire ont un accès illimité à Internet depuis leur chambre grâce au Wifi sur la base des données fournies par les enseignants dans les académies de Nanterre, de Bourges, ou du Val-d'Oise

S'agissant de l'information des parents, M. Serge Tisseron a estimé qu'il conviendrait d'impulser une grande campagne d'information dont le slogan pourrait être « 3, 6, 9, 12 ».

Le principe est certes un peu schématique mais à même de donner des repères : pas de télévision avant 3 ans ; pas de console de jeux personnelle avant 6 ans (beaucoup de travaux de neurophysiologie cérébrale montrent aujourd'hui que l'utilisation des dix doigts chez un enfant entre 3 et 6 ans est la condition d'énormes frayages cérébraux, or les consoles de jeux réduisent cette activité à 2 voire 4 doigts seulement) ; l'accès à Internet, accompagné d'un adulte, à partir de 9 ans (il faudrait sur ce point sensibiliser les parents sur le fait que l'introduction à Internet doit se faire avec un accompagnement) ; et enfin un usage individuel d'Internet à partir de 12 ans, puisqu'à partir de cet âge-là, les enseignants demandent aux élèves d'effectuer des travaux personnels sur Internet, sans que cela ne signifie pour autant une connexion illimitée en Wifi, nuit et jour.

Par ailleurs un véritable travail d'information doit être effectué, sur trois points :

– ce que l'on publie sur Internet y demeure éternellement (ce que beaucoup de parents ignorent et ne peuvent transmettre à leurs enfants) ;

– ce qu'on y met peut tomber dans le domaine public ;

– ce qu'on trouve ne doit pas être pris pour argent comptant (or beaucoup de parents sont prêts à croire ce qu'on trouve sur Internet et à laisser leurs enfants le croire).

Une campagne d'information doit être menée en direction des parents sur ces trois points, sur les tranches d'âges auxquelles introduire les nouvelles technologies ainsi que sur les grandes règles qui en régissent l'usage.

Cette campagne d'information pourrait être relayée par une campagne d'affichage, par la presse, Radio France et France Télévisions, notamment après 20 heures, où la loi du 5 mars 2009 a supprimé la publicité mais autorise la diffusion de messages d'intérêt général.

Mme Sophie Jehel, membre du conseil scientifique du Collectif interassociation Enfance et Médias (CIEM) a également souligné la nécessité de développer de véritables politiques publiques de prévention qui s'adressent à tous et pas seulement aux utilisateurs actifs d'Internet. Les élites politiques et associatives familières d'Internet doivent conserver à l'esprit que pour toucher un public large, notamment celui des milieux populaires, Internet ne peut suffire. Or, aujourd'hui, la plupart des politiques, des campagnes et des outils de prévention mis en place passent par Internet.

• Améliorer l'utilisation et la qualité des logiciels de contrôle parental

Selon Mme Sophie Jehel, les systèmes de filtrage parentaux ont été améliorés bien qu'aucune enquête nouvelle n'ait été conduite auprès des parents afin de comprendre les raisons pour lesquelles ils les utilisent si peu en réalité. Ces systèmes de filtrage sont essentiels, en l'absence d'autres moyens de régulation mais posent de nombreux problèmes pratiques. Les enquêtes montrent que 57 % des parents les ont installés mais, dans les faits, les deux enquêtes menées concluent que beaucoup les ont désactivés, sans que l'on s'interroge sur les raisons de ce choix.

Sans compter la difficulté qu'ils ont parfois à maîtriser ces outils informatiques, ou à accéder à l'information qui n'est pas suffisante, 61 % des parents, pourtant nombreux à souhaiter limiter le temps passé de leurs enfants sur Internet, ne savent pas qu'il est possible de restreindre le temps d'accès grâce au logiciel de contrôle parental (enquête IPSOS/e-Enfance, avril 2009).

Concernant plus spécifiquement le téléphone mobile, des actions ont été entreprises, notamment par l'AFOM (Association française des opérateurs mobiles). En dépit de cela, le nombre de parents qui utilisent le filtrage parental sur le téléphone mobile est encore plus faible, inférieur à 5 % selon les enquêtes disponibles.

M. Dominique Delorme, responsable de la ligne Net Écoute de l'Association e-enfance, a indiqué que l'association s'était impliquée dans le cadre des travaux de l'AFNOR (Association française de normalisation) afin de mettre

en place une norme permettant de tester les logiciels de contrôle parental que les fournisseurs d'accès à Internet ont l'obligation de fournir gratuitement. Toutefois on constate que beaucoup de parents les désinstallent, qu'ils sont de mauvaise qualité et que les fournisseurs d'accès ne respectent plus l'obligation de qualité de service. Or, a-t-il ajouté, il serait temps de trouver le budget nécessaire afin que cette norme devienne une véritable norme et que ces tests reprennent.

Mme Justine Atlan a relevé qu'une telle situation était d'autant plus déplorable que la France était, sur ce sujet, un leader à l'échelle européenne : elle est le seul pays qui ait réussi à contraindre les fournisseurs d'accès à offrir gratuitement à tous leurs clients un système de contrôle parental. Une chose fut de contraindre les fournisseurs à fournir de tels logiciels, une autre de faire en sorte que la gratuité ne soit pas synonyme de mauvaise qualité. Un suivi de la qualité du filtrage avait donc été mis en place pendant deux ou trois ans jusqu'à ce que l'on aboutisse à une volonté ministérielle de passer à des tests basés sur une véritable norme AFNOR. Toutefois cette initiative n'a pas été menée à son terme, ce qui est d'autant plus déplorable que cela fait deux années que les systèmes de contrôle parental fournis aux abonnés ne sont plus testés. On doit constater que la qualité de filtrage ne s'est pas améliorée.

M. Dominique Delorme a confirmé que ces discussions concernaient Internet mais également d'autres médias comme par exemple la téléphonie mobile. Il a affirmé que le filtrage sur la téléphonie mobile était inexistant. Le WAP (Wireless Application Protocole) par exemple n'est pas filtré, en dehors des contenus pornographiques pour lesquels le filtrage reste correct.

Mme Justine Atlan a indiqué, s'agissant du contrôle parental sur un téléphone mobile, qu'un groupe de travail réunissant l'ensemble des industriels avait été organisé au niveau européen sur la sécurité de l'enfance sur le mobile. Ce problème concerne plus directement les constructeurs et les plates-formes de téléphonie mobile puisque le contrôle parental doit être installé dans le téléphone lui-même et ne dépendra plus de l'abonnement fourni par l'opérateur.

La mission estime qu'il convient de mettre l'accent, dans le cadre de la campagne de communication et de sensibilisation, sur l'intérêt des logiciels de contrôle parental. Elle appelle de ses vœux un suivi précis de leur qualité et des raisons pour lesquelles les parents les utilisent si peu. Les fournisseurs d'accès à Internet pourraient participer, soit au travers de leur hotline, soit du financement de la ligne « Net écoute famille », à l'accompagnement des parents pour l'installation de leur logiciel de contrôle parental et la découverte de ses fonctionnalités.

Orientation n° 37 : renforcer le contrôle parental

Organiser une grande campagne d'information et de sensibilisation sur les technologies du numérique et le bon usage par les mineurs de ces dernières, basée sur le slogan « 3, 6, 9, 12 » : pas de télévision avant 3 ans ; pas de console de jeux personnelle avant 6 ans ; l'accès à Internet, accompagné d'un adulte, à partir de 9 ans ; et enfin un usage individuel d'Internet à partir de 12 ans.

Par ailleurs un véritable travail d'information doit être effectué, sur trois points :

– ce que l'on publie sur Internet y demeure éternellement ;

– ce que l'on y met peut tomber dans le domaine public ;

– ce que l'on y trouve ne doit pas être pris pour argent comptant.

Améliorer l'utilisation et la qualité des logiciels de contrôle parental.

C. LE RÔLE DES MÉDIAS

Le rapport de la Commission famille, éducation aux médias de mars 2009 avait estimé que se posait la question de « *l'offre destinée à la jeunesse, qui pour le CSA a toujours constitué un volet important de la protection de l'enfance. D'après une étude réalisée par S. Livingstone dans le cadre du projet « EU Kids Online », plus il existe une offre de programmes adaptés aux enfants, en télévision ou en ligne, plus les enfants se saisissent de cette offre et sont moins enclins à aller vers des activités à risques. Or les programmes jeunesse ne constituent actuellement que 20 % des programmes regardés par les 4-10 ans, et dans les 100 meilleures audiences réalisées sur cette population en 2008, six concernent des programmes déconseillés aux moins de 10 ans. Cet enjeu du maintien d'une offre adaptée en télévision, et de la vigilance des parents quant à la consommation de leurs enfants, est donc toujours très important.* »

Dans un rapport du 28 mars 2008 sur la programmation de France Télévisions, le CSA avait fait le constat que « *l'offre jeunesse de France Télévisions ne répondait qu'imparfaitement aux attentes que ce public et les parents sont en droit d'attendre* ». Cette dernière s'est réduite au fil des ans, sous la pression des exigences d'audience, pour s'uniformiser et se concentrer uniquement dans les matinées.

Pour offrir un large éventail de programmes consacrés à la jeunesse, tous les grands services publics européens ont profité de l'arrivée de la TNT pour lancer des chaînes dédiées. C'est le cas de la ZDF et de l'ARD en Allemagne, de la BBC en Grande-Bretagne, de la RAI en Italie et de la RTVE en Espagne.

Les programmes jeunesse sont en effet délaissés par les chaînes privées en l'absence d'enjeu publicitaire. C'est précisément parce que le marché publicitaire n'est pas suffisant sur cette cible que Gulli évolue de plus en plus vers une programmation de chaîne familiale, qui attire davantage les annonceurs.

1. Accroître l'offre du service public de l'audiovisuel sur tous les supports

La mission d'éducation aux médias de France Télévisions, inscrite dans son nouveau cahier des charges, et notamment celle de France 5, doit se traduire très concrètement, par exemple avec un magazine hebdomadaire autour de l'éducation aux médias, permettant de sensibiliser parents et enfants.

En outre, France 4 demeure, et à juste titre, la chaîne la plus critiquée pour son absence d'identité affirmée. Le nouveau cahier des charges la définit comme « *chaîne de la jeunesse et des nouvelles générations, dont la vocation est d'attirer et de fidéliser les jeunes et les jeunes adultes en exposant les nouveaux talents des scènes actuelles (musique et spectacle). Ses programmes proposent aux nouvelles générations un espace de partage et de reconnaissance* ». M. Rémy Pflimlin a, quant à lui, déclaré vouloir faire de la chaîne un « laboratoire d'idées »…

Dans l'hypothèse où la revente au groupe Lagardère des parts détenues par France Télévisions dans Gulli serait menée à son terme, la mission souhaite que soit envisagée la transformation de France 4 en chaîne spécifiquement dédiée à la jeunesse, totalement dépourvue de publicité.

Le groupe Lagardère, propriétaire à 66 % de Gulli, a en effet annoncé vouloir entrer en discussion avec France Télévisions en vue d'un rachat des parts du groupe public dans cette chaîne de la TNT gratuite. Rappelons que la chaîne jeunesse Gulli est détenue à 66 % par Lagardère et à 34 % par France Télévisions.

La mission estime qu'il s'agit là, et sans doute plus que jamais en raison des mutations de l'environnement médiatique, d'une mission incontestable du service public audiovisuel.

Cette proposition nous semble par ailleurs en totale cohérence avec le triple objectif de renforcement de la mission de service public de France Télévisions, de la réaffirmation de l'identité de la chaîne et de rajeunissement de l'audience du groupe.

La chaîne pourrait proposer des programmes et de messages destinés à sensibiliser les jeunes aux opportunités et aux risques d'Internet.

La mise en place de cette chaîne pourrait se prolonger sur le site Internet du groupe.

Orientation n° 38 : renforcer la mission d'éducation aux médias de l'audiovisuel public

Les études ayant montré que plus il existe une offre de programmes adaptés aux enfants, en télévision ou en ligne, moins ces derniers sont enclins à aller vers des contenus à risques, la mission préconise de faire de France 4 la chaîne jeunesse du groupe France Télévisions. Cette chaîne ne comporterait pas de publicité et proposerait notamment des programmes et des campagnes d'information permettant de sensibiliser les enfants, les adolescents et les jeunes adultes aux opportunités et aux risques liés au numérique.

2. Encourager au développement de contenus d'éducation aux médias sur les chaînes privées

Les médias privés devraient également jouer un rôle important en matière d'éducation aux médias.

Les chaînes de télévision et de radio privées pourraient définir un engagement annuel d'actions sur ce thème sous le contrôle du CSA. Les chaînes ayant un public particulièrement important d'enfants pourraient être spécifiquement incitées à produire des émissions d'éducation aux médias.

3. Encourager les jeunes à être créateurs de médias

M. Serge Tisseron a préconisé la création d'espaces publics sur Internet, considérant qu'on ne peut s'opposer aux pratiques problématiques qu'en encourageant les bonnes pratiques et Internet est justement un espace où des lieux devraient être créés par les communes, les départements, des espaces dans lesquels les jeunes pourraient publier leurs créations. Or, actuellement les jeunes n'ont pas d'autre possibilité, lorsqu'ils créent des images ou des vidéos, que de les publier sur *YouTube* ou sur *Facebook*. Ils perdent alors tout droit sur ces créations et désespèrent généralement de les voir tomber dans l'immense océan de réseaux sur lesquels personne ne les remarque.

Internet est ainsi un espace qui manque aujourd'hui en France de lieux de recueil et de valorisation fonctionnant de manière citoyenne, gratuite, sans déposséder de leurs droits ceux qui y mettent leurs productions. Il incombe au législateur d'encourager les collectivités territoriales à créer de tels espaces sur Internet.

Il serait, selon M. Serge Tisseron, utile de promouvoir, plus encore que les machinima [(1)] ou les pocket films [(2)], la création de jeux vidéos, ce qui là encore supposerait de créer des espaces dans lesquels des jeunes, encouragés à créer des jeux vidéos avec l'aide du secteur industriel, verraient leurs productions ne pas leur échapper puisqu'aujourd'hui, à moins de disposer de l'argent nécessaire à la création d'un site personnel sur Internet ou d'être soi-même informaticien, tout ce que l'on y publie devient propriété de l'espace sur lequel il est déposé. Ce que l'on publie sur *YouTube* appartient ainsi à *YouTube*. De la même façon, ce que l'on

(1) En tant que technique de production, le terme se réfère au rendu d'images de synthèse au moyen de moteurs 3D ordinaires (par opposition aux moteurs 3D complexes et supérieurs utilisés par les professionnels). Les moteurs de jeu vidéo tels que les jeux de tir subjectif sont beaucoup utilisés. Par conséquent, le rendu peut être effectué en temps réel, en utilisant un ordinateur personnel (soit celui du producteur, soit celui de l'utilisateur), plutôt que des moteurs 3D complexes nécessitant de gigantesques grappes de serveurs. Les machinimas sont un exemple des utilisations nouvelles et inattendues d'un jeu vidéo (comme la modification d'un tel jeu à des fins artistiques).

(2) Le pocket film est un moyen de s'exprimer en réalisant des fictions de poche. Avec le développement de la technologie permettant de recevoir, transmettre et d'enregistrer des images (fixes et mobiles) sur téléphone mobile, s'ouvre un nouveau champ d'exploration pour la création et l'écriture de l'image. L'arrivée des téléphones mobiles de dernières générations (3G) a permis de filmer, visionner des films sur son écran de téléphone, envoyer ses propres films sur d'autres téléphones ou les mettre en ligne sur Internet.

publie sur *Facebook* appartient à *Facebook*, y compris les droits dérivés. Si un jeune internaute crée sur *Facebook* une icône qui intéresse un annonceur, *Facebook* pourra la vendre sans que son auteur ne perçoive rien. L'absence d'espaces dans lesquels les créations des jeunes producteurs soient reconnues est donc aujourd'hui un important problème. M. Serge Tisseron a précisé que les jeunes sont d'ailleurs producteurs d'images de plus en plus tôt.

Orientation n° 39 : renforcer le rôle des médias dans l'éducation au numérique

– obliger les chaînes de télévision et de radio privées de définir un engagement annuel d'actions sur ce thème sous le contrôle du CSA ;

– encourager les jeunes à être créateurs de médias en mettant à leur disposition sur Internet des espaces publics dans lesquels ils pourraient publier leurs créations personnelles.

D. LE RÔLE DE LA CORÉGULATION

1. Au plan national

Le constat établi par le rapport de la Commission famille et éducation aux médias est que les ressources en éducation aux médias sont très parcellaires et éclatées. « *De nombreuses initiatives existent pourtant en la matière, portées par l'Éducation nationale, au travers notamment du Centre de liaison de l'enseignement et des médias d'information (CLEMI), par des associations éducatives, des associations de parents d'élèves et des associations dédiées à la protection de l'enfance, ou par les institutions publiques de l'audiovisuel, France Télévisions, l'Institut national de l'audiovisuel (INA) ou encore les instances comme le Conseil supérieur de l'audiovisuel (CSA) et le Forum des droits sur l'Internet (FDI), des initiatives européennes comme « Internet plus sûr », l'adoption d'une Charte des sites communautaires, le lancement d'un appel d'offres pour un numéro d'information aux familles (en France, le service Net écoute Famille ... Ces initiatives ne sont pas assez relayées, pas assez coordonnées et ne constituent pas une offre lisible et accessible pour toutes les familles* ».

La rapporteure, Mme Agnès Vincent-Deray, estimait que « *Les marges de progrès sont donc importantes, notamment dans le sens du renforcement de la co-régulation que pratique actuellement le FDI. (...) Les travaux et recommandations du FDI depuis 2003 ont permis de façonner des réponses collectives entre les pouvoirs publics et les entreprises, mobilisant les outils régulatoires de chacun. Ainsi, se sont développées des politiques de filtrage parental, d'information des internautes, de contrôle de l'âge…. Ces outils sont importants et ne cessent de progresser* (…) »

Les travaux du Forum des droits sur Internet sur la publicité ciblée ont abouti à la signature d'une charte très importante **«** Publicité ciblée et protection

des internautes », signée le 30 septembre 2010 par dix associations professionnelles réunissant annonceurs, régies publicitaires, moteurs de recherche, boutiques en ligne… Mme Véronique Fima-Fromager a rappelé que la charte signée sous l'égide de la secrétaire d'État à l'économie numérique, Mme Kosciusko-Morizet, préconisait l'interdiction du ciblage pour les moins de treize ans. Elle a estimé qu'il serait souhaitable que cette limite d'âge soit portée à dix-huit ans.

Mme Sophie Jehel, membre du conseil scientifique du Collectif interassociation Enfance et Médias (CIEM) a estimé que la régulation d'Internet devait associer l'ensemble des acteurs concernés, afin de mettre en place une véritable co-régulation tripartite (opérateurs, pouvoirs publics nationaux et européens, et associations représentatives des parents et des éducateurs). La co-régulation implique d'être en mesure de veiller à l'efficacité des mesures prises et à la qualité d'une information efficace, en créant des lieux de consultation et de rencontre régulière, réunissant les différents groupes impliqués, afin qu'ils expriment leurs attentes et leurs demandes.

La Commission famille et éducation aux médias avait préconisé la création d'une fondation *ad hoc*.

Orientation n° 40 : confier au Conseil national du numérique un rôle ambitieux de corégulation en matière de prévention et d'éducation aux médias

La mission estime qu'il incomberait à un Conseil national numérique reconfiguré selon les préconisations formulées dans la dernière partie du présent rapport de se saisir de la question prioritaire de la prévention et de l'éducation aux médias en réunissant les institutions publiques, les associations, les chercheurs, les professionnels des médias et des réseaux (télévisions et radios publiques comme privées, fournisseurs d'accès à Internet, sites et portails Internet…).

Au-delà de la mission d'élaboration et de suivi des chartes de bonne conduite, la mission du Conseil serait multiple :

– assurer une veille sur les actions d'éducation aux médias et constituer un Observatoire des usages des technologies numériques par les mineurs ;

– créer un portail consacré à l'éducation aux médias, rassemblant les ressources utilisées sur tous les supports ; faire émerger des ressources validées d'éducation aux médias, disponibles pour le plus grand nombre ; soutenir des actions, d'information, de communication, notamment des différents médias, des collectivités, des associations ;

– contrôler l'élaboration de systèmes de contrôle parental simples et de qualité et assurer un suivi de l'utilisation qui en est faite par les parents ;

– être un lieu de dialogue entre l'ensemble des acteurs.

S'agissant de la charte sur la publicité ciblée, la mission souhaite que l'interdiction du ciblage, qui concerne actuellement les moins de treize ans, soit élargie aux moins de seize ans.

2. Au plan européen

Premier du genre, un accord européen ayant pour objectif de favoriser un usage protégé du Web 2.0 a été signé en février 2009, dans le cadre de la Journée pour un Internet plus sûr organisée par la Commission européenne.

À la demande de la Commission européenne, dix-sept sites de socialisation, recouvrant des pratiques très diverses, allant du site communautaire comme *Facebook* au site de partage de vidéos comme *YouTube* ou encore à la plate-forme de blogs comme *Skyblog*, ont signé un accord portant sur la protection des jeunes internautes.

Les principaux engagements pris à la demande de la Commission européenne sont nombreux et divers : signaler un abus en un seul clic ; paramétrer par défaut comme « privés » les profils et les listes de contacts des internautes mineurs et verrouiller leur accès (impossible directement à partir du site comme via un moteur de recherche) ; rendre plus visibles les options de vie privée permettant de réserver à ses amis l'accès à certaines informations mises en ligne ; empêcher, grâce à un mode d'inscription trop complexe, les enfants trop jeunes d'utiliser leur site.

Parmi les signataires de cet accord, se trouvent les grands acteurs du Web, Dailymotion, *Facebook*, *YouTube*, Microsoft Europe, *MySpace*, *Yahoo !*, *Skyrock*, *Bebo* et des moins connus comme *Netlog*, *Arfo*, *Giovanni.it*, *Hyves*, *Nasza-kiaza.pl*, *One.it*, *StudiVZ*, *Suiake/Habbo Hoel* et *Zap.lu*. Cet accord a été rendu possible grâce aux travaux d'un groupe, la *Social Networking Task Force,* établie par la Commission en avril 2008, réunissant des sites de socialisation, des ONG et plusieurs chercheurs. Selon Mme Viviane Reding, commissaire européenne à la société de l'information et aux médias, il s'agit là d'un bon exemple d'autorégulation d'un secteur d'activité, à laquelle la Commission européenne est particulièrement favorable.

Malgré la signature de cette charte, la mission d'information a constaté que les réseaux sociaux ne contrôlaient pas suffisamment l'âge que les mineurs déclarent lorsqu'ils s'inscrivent. M. Marc Zuckerberg, président et fondateur de *Facebook* avait envisagé d'abaisser encore l'âge minimum requis pour l'ouverture d'un compte *Facebook* avant de confirmer son maintien à 13 ans, mais sans exclure un abaissement ultérieurement.

La mission déplore que l'entreprise *Facebook* mette aussi peu de diligence et de responsabilité à protéger les enfants qu'elle en a mis à répondre aux questions de notre mission sur l'ensemble de ces sujets. Or, malgré la difficulté technique de procéder à un contrôle systématique et préalable de l'âge des utilisateurs, il lui est loisible de renforcer l'information sur cette interdiction et de procéder à des contrôles réguliers et à des annulations de comptes lorsqu'il s'avère qu'un membre a de toute évidence moins de 13 ans.

Orientation n° 41 : renforcer la corégulation au plan européen en mettant l'accent sur plusieurs priorités :

– agir de façon concertée pour contraindre les réseaux sociaux à appliquer plus strictement l'interdiction de s'inscrire avant un certain âge. La mission déplore que l'entreprise *Facebook* mette aussi peu de diligence et de responsabilité à protéger les enfants qu'elle en a mis à répondre aux questions de notre mission sur l'ensemble de ces sujets. Or, malgré la difficulté technique de procéder à un contrôle systématique et préalable de l'âge des utilisateurs, il lui est loisible de renforcer l'information sur cette interdiction et de procéder à des contrôles réguliers ainsi qu'à des annulations de comptes lorsqu'il s'avère qu'un membre a de toute évidence moins de 13 ans ;

– obtenir des engagements clairs des opérateurs, des hébergeurs et des éditeurs de site (sur le modèle de la Charte des sites communautaires signée au niveau européen) sur l'information qu'ils sont prêts à mettre en place, en ce qui concerne la protection des mineurs et plus généralement leur responsabilité sociale vis-à-vis des jeunes. Ces messages d'information ne devraient pas seulement être bien exposés sur les sites Internet, à des emplacements visibles et accessibles, ils devraient également être envoyés aux internautes lors de l'ouverture d'une adresse de courriel par tous les FAI (fournisseur d'accès à Internet) et les hébergeurs de boîtes de courriels, accompagner tout logiciel de contrôle parental et s'afficher lors de l'ouverture d'un blog ou d'un compte sur un réseau social. M. Thomas Jarzombek, député allemand, président, au sein de la commission d'enquête mise en place par le *Bundestag*, des groupes de travail sur la protection des mineurs et l'éducation aux médias, a souligné, s'agissant de la protection des mineurs sur les réseaux sociaux, l'efficacité des campagnes d'information à l'aide de la « communication virale » [(1)]. Il a indiqué que de telles campagnes avaient permis de lancer avec succès des messages d'avertissement en direction des jeunes filles qui mettent sur Internet des photos d'elles-mêmes en petite tenue. Plus de la moitié des utilisateurs aurait modifié son comportement suite à cette initiative. Il conviendrait par conséquent d'inciter les grands acteurs d'Internet à se mettre d'accord pour lancer ce type de campagnes d'information ;

– l'effort d'information pourrait aussi concerner le signalement des contenus choquants ou incitant à des comportements à risque. Aujourd'hui, les pages de signalement des contenus choquants ne sont pas toujours facilement accessibles et sont parfois assez complexes, avec des formulaires à remplir. Ces pages pourraient être accompagnées d'une vidéo de démonstration pour que leur usage soit facilité.

En conclusion, construire une véritable co-régulation des services numériques apparaît comme une priorité. Les outils et l'information actuellement mis en place sur Internet ne peuvent suffire à garantir une action efficace à l'égard des jeunes et de leurs parents : il est nécessaire d'impliquer et d'engager, dans une démarche de co-régulation, l'État, les entreprises et la société civile. Ce point est développé dans la dernière partie du présent rapport consacrée au Conseil national du numérique.

(1) Les messages sont transmis de proche en proche par les utilisateurs. Cette technique est utilisée par le marketing et passe essentiellement par les réseaux sociaux.

TITRE TROISIÈME

LE DROIT À L'ACCÈS À INTERNET

PREMIÈRE PARTIE : QUELLE NEUTRALITÉ DE L'INTERNET ?

Comme l'a souligné M. Philippe Logak, secrétaire général de SFR, lors de son audition par la mission le 8 juin 2010, le sujet de la neutralité du net entre pleinement dans le champ de réflexion de la mission d'information sur les droits de l'individu dans la révolution numérique. Réfléchir à la neutralité du net, c'est en effet s'interroger sur les modalités concrètes de mise en œuvre d'un droit désormais consacré, celui d'accéder à Internet. Consacrer un principe de neutralité de l'Internet ne va cependant pas de soi. La neutralité du net ne fait d'ailleurs pas partie de la déclaration finale de l'e-G8 Forum qui a eu lieu à Paris les 24 et 25 mai 2011. Les positions, y compris au sein même des États, sont actuellement beaucoup trop opposées. Le premier problème soulevé par la neutralité de l'Internet est d'ailleurs la très grande confusion qui entoure cette notion, dont les contours sont mal définis et les acceptions aussi nombreuses que les débats qu'elle suscite.

I. LA NEUTRALITÉ DE L'INTERNET : UNE NOTION QUI RECOUVRE PLUSIEURS DÉBATS DE NATURE DIFFÉRENTE

Tim Wu, universitaire américain considéré comme le « père » de cette terminologie, la définit comme suit[(1)] : « *Pour qu'un réseau public d'information soit le plus utile possible, il doit tendre à traiter tous les contenus, sites et plateformes de la même manière. [...] Internet n'est pas parfait mais son architecture d'origine tend vers ce but. Sa nature décentralisée et essentiellement neutre est la raison de son succès à la fois économique et social.* »

La notion de neutralité du net renvoie donc à l'idée que, d'un point de vue technique, toutes les données sont transportées et traitées de la même manière, de leur point d'origine jusqu'à leur destination finale. La neutralité du réseau serait ainsi remise en cause par toutes les pratiques de blocage de la transmission de données, de dégradation ou de ralentissement du trafic.

L'ouverture de l'Internet est considérée comme un des facteurs essentiels de son succès et de son développement. Elle a en effet permis aux utilisateurs, où qu'ils se trouvent, de développer des applications, des services ou des contenus et de les rendre immédiatement accessibles à la communauté des internautes.

Horizon vers lequel l'Internet doit tendre ou mythe fondateur de ce dernier, la neutralité du réseau exigerait en toute rigueur une non-discrimination parfaite dans l'acheminement du trafic et un traitement équivalent de tous les parquets d'informations sur le réseau.

---

(1) Extrait d'un article intitulé « Network Neutrality, Broadband Discrimination » dans « Open architecture as communications policy *», Center for Internet and Society, Stanford Law school, 2004.*

Or, lors de son audition du 22 juin 2010, M. Yves Le Mouël, directeur général de la Fédération française des télécoms (FFT), a rappelé à la mission qu'une neutralité parfaite n'avait jamais existé. Le réseau a toujours fait l'objet d'un « management » du seul fait qu'une identité est attribuée à chaque paquet de données. Les impératifs de la gestion du trafic (lutte contre les virus, les spams et les attaques informatiques, nécessité de maintenir une qualité de service acceptable en cas de congestion etc.) obligent en outre les opérateurs à pratiquer certaines discriminations.

C'est pourquoi, certains, comme M. Stéphane Richard, directeur général de France Télécom/Orange, entendu par la mission le 22 juin 2010, préfèrent l'expression « Internet ouvert » à celle de « neutralité du réseau ».

De surcroît, la notion de neutralité de l'Internet recouvre en réalité plusieurs débats, soulevés par plusieurs évolutions de nature totalement différente susceptibles de la remettre en cause.

A. LE DÉBAT SUR LES CONDITIONS DE LA GESTION DE L'ACCROISSEMENT DU TRAFIC ET LA RÉPARTITION DES COÛTS ENGENDRÉS PAR CE DERNIER

Jusqu'à présent, les opérateurs télécoms financent seuls la construction des réseaux grâce aux abonnements acquittés par les consommateurs.

Or, depuis le début des années 2000, le trafic sur Internet a connu une croissance exponentielle, d'abord sous l'effet du développement du *peer-to-peer*, puis de la vidéo. Cette évolution soulève des questions techniques liées à la gestion du trafic sur le réseau mais aussi des questions d'ordre économique portant sur la répartition des coûts engendrés par ce dernier entre les différents acteurs de l'Internet.

Il convient d'emblée de souligner que le risque de saturation des réseaux à court terme, invoqué par les fournisseurs d'accès à Internet à l'appui de la mise en place de mesures de gestion du trafic, est contestée ou nuancée par d'autres observateurs.

Parallèlement, ces dernières années, la valeur ajoutée de l'écosystème Internet s'étant déplacée des fournisseurs d'accès vers les éditeurs de contenus, les premiers ont eu tendance à investir le segment des seconds, ce qui entraîne des phénomènes de concentration verticale. La conséquence est que chacun, sur un marché donné, est tenté de favoriser ses services sur un autre marché par rapport à ses concurrents, et donc de restreindre à cet effet l'accès au réseau de ces derniers. Cette pratique, de nature discriminatoire, est contraire au principe de neutralité.

En France, le risque de discrimination est réel dans la mesure où les opérateurs de télécommunications, à l'instar de France Télécom qui domine le marché français de l'accès à Internet, proposent des offres de contenus ou de

services et sont même devenus producteurs. En l'absence de règles, ils pourraient être encouragés à privilégier leurs propres offres.

Le premier cas de « gestion de trafic » ayant soulevé la question de la neutralité d'Internet en France remonte à août 2007, lorsque le fournisseur d'accès Neuf Cegetel a été accusé de volontairement brider l'accès au site de partage de vidéos *Dailymotion* en raison de la forte consommation en bande passante des usagers de ce site. Le problème a connu une résolution rapide. Quelques jours après l'« incident », le blog officiel de Dailymotion affichait le message suivant : « *Les abonnés de Neuf ont pu faire l'expérience de quelques lenteurs sur le site de* Dailymotion *entre jeudi et dimanche dernier. Ces désagréments ont pour origine une perturbation dans la gestion de l'échange de trafic entre Neuf et* Dailymotion*. Depuis lundi 13 août tout est revenu dans l'ordre et le site est de nouveau accessible pour les abonnés de Neuf.* »

Si les fournisseurs de contenus admettent la possibilité que les opérateurs de réseaux pratiquent différents tarifs pour leurs abonnés en fonction de la qualité du service offert, ou distribuent en priorité certains types de services pour des considérations techniques, ils redoutent en revanche d'être victimes de pratiques anticoncurrentielles, dans l'hypothèse où les opérateurs privilégieraient leurs propres partenaires ou leurs propres filiales de vidéo à la demande par exemple. Ainsi, les internautes pourraient-ils ne pas avoir accès aux mêmes sites et aux mêmes contenus selon le fournisseur d'accès choisi.

Alors que la tentation est grande pour les fournisseurs d'accès à Internet de mettre en place une gestion différenciée des services dans le but de les « monétiser », de vifs débats politiques ont lieu pour déterminer si et dans quelle mesure le principe de neutralité doit être garanti par la législation.

Les entreprises de l'Internet défendent trois principes : la non-discrimination dans l'accès aux contenus du net, la transparence de la gestion du réseau et l'arbitrage des litiges qui pourraient survenir entre fournisseurs de services et fournisseurs d'accès par l'autorité de régulation des postes et des télécommunications.

Lors de son audition du 22 juin 2010, M. Stéphane Richard, directeur général de France Télécom/Orange, a rappelé que la forte augmentation du trafic sur les réseaux Internet mobile et fixe posait des difficultés de gestion de ce trafic sur des infrastructures nécessairement limitées. C'est pourquoi il a mis en garde contre l'invocation de « grands principes philosophiques, tels que le droit d'accès universel au réseau » qui pourrait faire perdre de vue les risques très prosaïques de congestion auxquels les opérateurs doivent faire face.

Il a rappelé que la solution, envisagée par la majorité des opérateurs à travers le monde, pourrait être la discrimination, non pas par le contenu, mais par la qualité de service et le tarif, les opérateurs proposant différentes formules d'accès à Internet à des prix variables suivant la qualité de service proposée.

Entendu le 8 juin 2010 par la mission, M. Emmanuel Forest, vice-président, directeur général délégué de Bouygues Télécom a lui aussi défendu l'idée selon laquelle les opérateurs devaient pouvoir être rémunérés pour la qualité de service qu'ils offrent. L'utilisateur qui, sur son *smartphone*, se connecte en continu au réseau pour visionner des chaînes de télévision, utiliser *YouTube* ou des services en *streaming* (1), ne doit, selon lui, pas en être empêché, sous réserve d'acquitter un prix d'abonnement correspondant aux investissements qu'une telle connexion exige de la part de l'opérateur, notamment dans la boucle locale radio (2). À l'inverse, l'utilisateur qui se contente de synchroniser des courriels et fait un usage plus épisodique des multiples services disponibles sur Internet doit pouvoir acquitter un prix moindre.

Entendu le 16 juin 2010 par la mission, M. Pierre Danon, président-directeur général de Numéricable-Completel, a indiqué que sur le réseau de Numéricable, 5 % des abonnés utilisaient 55 % de la bande passante et qu'une étude détaillée avait permis de mettre en évidence que ces 5 % d'utilisateurs téléchargaient sur Internet l'équivalent de 850 films de longue durée par mois en moyenne.

Ces téléchargements excessifs ne sauraient, aux yeux de M. Pierre Danon, témoigner d'un usage responsable et avisé du réseau. Ces utilisateurs paient leur forfait Internet au même prix que les internautes qui font un usage plus raisonnable d'Internet. Or, la surconsommation des premiers ralentit et parasite le trafic au détriment des seconds.

À cet égard, Numéricable s'est dit favorable à une modulation du trafic suivant la consommation en bande passante par l'internaute : dès lors que ce dernier aurait une consommation excessive, il verrait son débit réduit. Cette limitation du débit, dans certains cas avérés d'abus de la part de l'utilisateur, ne constituerait pas, selon lui, une atteinte aux droits et libertés de l'internaute, dans la mesure où elle ne porterait que sur le volume en bande passante et non sur le contenu.

M. Emmanuel Forest a indiqué que la Fédération française des télécoms (FFT) travaillait à l'élaboration d'une charte qui redéfinirait les principes d'un Internet ouvert à tous, sans discrimination, et d'une offre de service de qualité, adaptée aux besoins de chaque utilisateur et passant par une gestion adaptée du réseau dans l'intérêt de l'ensemble des internautes.

Selon M. Yves Le Mouël, directeur général de cette même Fédération, entendu le 22 juin 2010, l'une des difficultés est que les utilisateurs ont pris l'habitude, en France, de disposer d'un prix d'accès très bon marché, de l'ordre de 30 euros, aux offres *triple play* (Internet, télévision, téléphone) permettant l'accès

---

(1) Diffusion en mode continu.

(2) La boucle locale radio (BLR) est « l'ensemble des technologies permettant à un particulier ou une entreprise d'être relié à son opérateur (téléphonie fixe, Internet, télévision...) via *les ondes radio. C'est un type de boucle locale qui permet de compléter la desserte filaire traditionnelle. » (source :* Wikipedia*).*

illimité à Internet, c'est-à-dire indépendamment du trafic consommé, alors même qu'un trafic plus important engendre des coûts.

Depuis juin 2010, il semblerait que le marché soit déjà en train de remettre en cause ce standard. L'évolution de l'offre des opérateurs de téléphonie mobile pour l'accès à Internet semble indiquer qu'à l'avenir l'illimité sera l'exception plutôt que la règle.

En effet, l'abandon le 1er janvier 2011 du taux réduit de TVA à 5,5 %, instauré en 2007, sur la moitié du montant des forfaits d'accès Internet *triple play* pour la partie concernant l'acheminement de services de télévision, ainsi que sur certains forfaits mobiles donnant accès à Internet et donc à des services audiovisuels à la demande, a été l'occasion, pour les opérateurs français, d'abandonner le standard du *triple play* à 30 euros par mois instauré par Free en 2003. Les fournisseurs d'accès à Internet par ADSL, Orange, SFR, Free et Bouygues Télécom, ne se sont pas contentés d'augmenter le prix du forfait *triple play* du montant de la hausse de la TVA. Ils ont également profité de cette occasion pour décliner leurs offres et mettre fin à l'uniformisation tarifaire. En optant pour cette solution, les opérateurs incitent le consommateur à choisir des forfaits en fonction des performances proposées et des services fournis.

S'agissant de la répartition des coûts engendrés par l'accroissement du trafic sur les réseaux, M. Emmanuel Forest a estimé que les fournisseurs de services Internet pourraient contribuer aux investissements dans les réseaux, soit par le biais d'une participation financière consistant à acheter à l'opérateur de réseau les capacités de transmission et la qualité de service qu'il souhaite pour ses clients, soit par la voie d'une charte ou d'un label de bonne utilisation des réseaux. Il a souhaité que l'ensemble de ces actions se fasse dans le cadre d'une autorégulation, sans intervention d'une législation qui, au regard de technologies et de besoins très évolutifs, risque toujours d'être trop rigide.

M. Stéphane Richard a lui aussi jugé qu'à l'heure actuelle, la responsabilité des différents acteurs n'était pas très satisfaisante puisqu'elle ne pesait que sur les opérateurs chargés d'investir pour accroître la capacité des réseaux, ceux qui font le trafic sur ces derniers estimant en être, pour leur part, exonérés. Un rééquilibrage apparaît donc selon lui nécessaire afin qu'il y ait une prise en charge plus collective des problèmes de congestion des réseaux.

M. Maxime Lombardini, directeur général d'Iliad-Free, auditionné le 8 juin 2010 par la mission, a indiqué que Free se préoccupait aussi des relations avec les fournisseurs et éditeurs de services sur Internet, avec lesquels, pendant longtemps, les relations ont été équilibrées. Depuis quelques années, cependant, Free assiste à une très grande concentration du trafic sur quelques grandes plates-formes, « agrégateurs » de flux (tels que *Google* avec *YouTube*). Par ailleurs, le poids croissant de la vidéo oblige Free à mettre en œuvre des capacités quasiment sans limites pour assurer le maintien du trafic. La position de Free sur la neutralité du net est donc claire et connue. Il n'est pas question de restreindre l'accès à un

service ; la société souhaite simplement pouvoir facturer à ces plates-formes les capacités additionnelles mises en œuvre, au-delà d'un certain niveau de trafic. L'objectif est de ne pas avoir une contribution sans limites de ceux qui construisent les réseaux au bénéfice de plates-formes qui ne s'en préoccupent pas. Selon M. Maxime Lombardini, il n'apparaît pas nécessaire de légiférer sur ce point, mais plutôt d'adopter des « codes de bonne conduite », avec des engagements de transparence sur les conditions économiques de cette facturation.

LE DÉBAT SUR LA NEUTRALITÉ DU NET AUX ÉTATS-UNIS

La neutralité du net fait l'objet d'une véritable bataille politique aux États-Unis. Sa protection figurait parmi les promesses de campagne du Président Obama.

Sur la neutralité du net comme sur la protection de la vie privée, les rapporteurs, au cours de leur déplacement à Washington début février 2011, ont constaté que le débat portait sur la légitimité, l'opportunité et les modalités de l'intervention publique, la plupart des interlocuteurs rencontrés jugeant l'autorégulation et la mise en place de « bonnes pratiques » préférables au recours à la loi, l'intervention de la puissance publique n'étant jugée légitime que si une « défaillance du marché » (« *market failure* ») avait été constatée. En outre, l'accent est mis sur la difficulté de réguler un environnement qui connaît un développement et des mutations technologiques extrêmement rapides.

Les règles votées le 21 décembre 2010 par la *Federal Communications Commission* (FCC) constituent pourtant un compromis entre les partisans de la neutralité du net et les intérêts des opérateurs. Mme Mignon Clyburn, Commissaire de la FCC, a reconnu que ces règles étaient « légères » et « très différentes de ce qui avait été envisagé à l'origine ». M. Darrell West, spécialiste de ces questions à la *Brookings Institution* a estimé que l'administration Obama n'avait pas tenu ses promesses de campagne.

Après plusieurs mois de consultations, le collège des commissaires de la FCC a en effet voté, le 21 décembre 2010, la mise en place de règles limitées sur la neutralité d'Internet. Le texte voté interdit aux fournisseurs d'accès à Internet (FAI) de bloquer l'accès à certains sites ou services, sans empêcher les opérateurs de facturer des tarifs plus élevés à ces sites en contrepartie d'un accès de meilleure qualité des internautes à leur contenu (« *paid prioritization* »). Avec ces règles, les FAI pourraient donc théoriquement exiger des sites qui génèrent beaucoup de trafic, comme *YouTube* ou *Amazon*, qu'ils paient des frais supplémentaires pour le maintien d'une qualité de service égale. Le texte de la FCC met cependant en garde les opérateurs contre toute « *discrimination déraisonnable* ».

Ces règles ne s'appliquent pas aux réseaux mobiles, une exception que la FCC justifie en mettant en avant l'évolution rapide des technologies mobiles et le volume limité de données pouvant être véhiculé sur ces réseaux. Si les opérateurs mobiles sont donc essentiellement soumis à une obligation de transparence, le texte leur interdit néanmoins de bloquer certaines applications concurrentes de leurs propres services, dont Skype.

Si la Maison Blanche soutient formellement les règles édictées par la FCC, beaucoup d'interlocuteurs ont fait part de leurs réserves. Plusieurs faiblesses mineraient ainsi les règles de la FCC : exemption des réseaux sans fil et des moteurs de recherche de leur champ d'application, possibilité maintenue d'accorder la priorité à certaines applications.

L'entreprise *Verizon* conteste devant les tribunaux la compétence de la FCC pour édicter de telles règles et le Congrès, à majorité républicaine, souhaite les faire supprimer. Ces actions vont ralentir considérablement le dossier.

Au Congrès, le débat sur neutralité du net donne lieu à un affrontement idéologique entre les partisans du libre marché et ceux de la régulation.

Pour les républicains rencontrés, aucune mesure destinée à garantir la neutralité du net ne devrait être prise sans preuve préalable des insuffisances du marché. M. Neil Fried, membre de

l'équipe du représentant Greg Walden (Oregon), nouveau président du comité de l'Énergie et de l'industrie, reproche à la FCC de n'avoir pas conduit « d'analyse du marché » avant de mettre en place ses règles.

Selon le représentant Bob Goodlatte (Virginie), toute régulation serait nuisible à l'innovation et les lois antitrust permettaient déjà de gérer d'éventuelles dérives. Comme d'autres opposants à la neutralité du net, M. Neil Fried dénonce également une focalisation excessive sur cette question, au détriment d'autres problèmes comme « la neutralité des moteurs de recherche ».

Au contraire, à l'*Information Technology and Innovation Foundation* (ITIF), Rob Atkinson a souligné que « l'Internet n'a jamais été neutre » et que la gestion du réseau est indispensable à l'heure où « 5 % des internautes utilisent 90 % de la bande passante ».

De leur côté, les démocrates (équipe du sénateur Rockefeller, président du comité de l'Industrie, de la science et des transports) paraissent confiants sur la pérennité des règles énoncées par la FCC, le Président Obama s'étant engagé à opposer son veto à tout projet de loi visant à les remettre en cause. Ils notent toutefois que la FCC pourrait bien perdre le procès que lui a intenté Verizon, car sa compétence juridique sur cette question est contestée. Pour M. Aneesh Chopra, *Chief Technology Officer* de la Maison Blanche, avec les règles édictées par la FCC, le problème de la neutralité du net doit être considéré comme réglé.

B. LE DÉBAT SUR LE DÉVELOPPEMENT DU BLOCAGE ET DU FILTRAGE LÉGAUX

Dans son rapport sur la neutralité du net remis au Parlement le 16 juillet 2010 en application de l'article 33 de la loi n° 2009-1572 du 17 décembre 2009 relative à la lutte contre la fracture numérique, le Gouvernement évoque la question du « *traitement différencié de certains flux pour respecter des obligations légales* » en constatant que « *sur l'Internet, comme ailleurs, les agissements illicites (fraudes et escroqueries, délits de presse, atteintes à la vie privée, contrefaçon, piratage des œuvres protégées par le droit d'auteur, diffusion de contenus pédopornographiques, etc.) doivent être poursuivis et sanctionnés, ce qui peut impliquer la mise en place de dispositifs de filtrage ou de blocage de certains contenus.* »

Ce constat est pourtant loin d'être partagé et la question fait l'objet de vives controverses en France. Si la nécessité de lutter contre les contenus illégaux, en particulier les contenus odieux tels que la pédopornographie, ne fait pas débat, ce dernier porte sur l'opportunité et la légitimité d'y parvenir par la mise en place de dispositifs de filtrage et de blocage.

Pour faire retirer un contenu illégal, l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (« LCEN ») prévoit en effet un régime de responsabilité en cascade selon lequel il convient de solliciter d'abord l'éditeur, puis l'hébergeur du contenu, avant de se tourner vers les fournisseurs d'accès à Internet, comme solution de dernier recours, en cas d'échec des demandes précédentes.

Les diverses mesures de filtrage et de blocage remettent en cause ce principe de subsidiarité.

Le débat législatif sur les mesures obligatoires de filtrage avait d'ailleurs fait son apparition à l'occasion de l'examen de la LCEN qui donnait au juge la possibilité d'exiger des fournisseurs d'accès à Internet qu'ils prennent toutes mesures propres à faire cesser un dommage occasionné par un service de communications au public en ligne et qu'ils suspendent l'accès à un contenu violant le droit d'auteur. La présidente de la commission des Affaires culturelles et de l'éducation, Mme Michèle Tabarot, alors rapporteure pour avis de la commission des Lois de l'Assemblée nationale, à laquelle avait été renvoyé l'examen des articles relatifs aux mesures de blocage, avait souligné l'inefficacité partielle de ces mesures sur un plan technique, les possibilités de contournement ainsi que la plus grande efficacité de la suppression du contenu à la source, justifiant le principe de subsidiarité suivant lequel des mesures visant à empêcher l'accès aux contenus doivent d'abord être imposées aux éditeurs et hébergeurs de ces contenus avant d'être imposées aux fournisseurs d'accès à Internet.

La légitimité et les conditions dans lesquelles un internaute peut se voir privé de son accès à Internet ont été abondamment débattues à l'occasion de l'examen de la loi favorisant la diffusion et la protection de la création sur Internet, dite loi « HADOPI I ». Le Conseil constitutionnel a tranché, dans sa décision n° 2009-580 DC du 10 juin 2009, en considérant que les pouvoirs de sanction institués par les dispositions déférées habilitaient la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à Internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'était pas limitée à une catégorie particulière de personnes mais s'étendait à la totalité de la population ; que ses pouvoirs pouvaient conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins. Une telle coupure de l'accès à Internet ne pouvait donc être prononcée que par l'autorité judiciaire.

Après les débats suscités par la question de la suspension de l'accès à Internet prévue par les lois « HADOPI » précitées, le débat a ressurgi à l'occasion de l'examen de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne qui prévoit un mécanisme de blocage de l'accès aux sites de jeux en ligne non agréés. S'est alors posée la question de la possibilité d'instituer une procédure de blocage administrative sans passer par le juge.

Enfin, l'examen de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (loi dite « LOPPSI 2 ») a donné lieu à d'intenses débats sur l'opportunité d'instituer des mesures de blocage des contenus pédopornographiques et, dans une telle hypothèse, sur la nécessité d'une intervention du juge pour prononcer ces mesures,

la solution retenue reposant finalement, et contrairement à la loi sur les jeux en ligne, sur la décision de la seule autorité administrative, solution validée par le Conseil constitutionnel dans sa décision n° 2011-625 DC du 10 mars 2011. Considérant que la « LOPPSI » « *ne confère à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'Internet, l'accès à des services de communication au public en ligne lorsqu'et dans la mesure où ils diffusent des images de pornographie infantile ; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé* » le Conseil a estimé que ses dispositions assuraient « *une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789* ».

C. LE QUESTIONNEMENT SUR LA NEUTRALITÉ DES PRATIQUES DE L'ENSEMBLE DE LA CHAÎNE DE VALEUR D'INTERNET ET NOTAMMENT DES MOTEURS DE RECHERCHE

Les problématiques liées à la neutralité du Net débordent largement la seule neutralité de l'acheminement des données pour concerner :

— *les téléphones mobiles*. L'accès à certaines applications peut y être favorisé (par exemple l'accès à l'Apple store sur l'Iphone d'Apple), et certains logiciels au contraire écartés (il n'y a par exemple pas de technologie *flash* [(1)] sur les Iphones) ;

— *les moteurs de recherche*. Le caractère objectif du référencement et de la présentation des résultats par ces derniers fait débat, d'autant que le moteur *Google* représente à lui seul les deux tiers des recherches ;

— *les télévisions connectées*. Des partenariats entre constructeurs de télévisions et éditeurs de contenus (par exemple entre Sony et *Google*) prévoient d'ores et déjà des clauses d'exclusivité, qui font craindre des modèles fermés préjudiciables aux consommateurs.

II. LES ÉVOLUTIONS PRÉCONISÉES PAR LA MISSION

A. QUEL CADRE POUR LA GESTION DE TRAFIC ?

La mission souhaite que soit préservé un Internet libre et ouvert, c'est-à-dire un Internet qui offre la possibilité à tout utilisateur :

(1) Flash Player, développé et distribué par Macromedia (racheté en 2005 par Adobe Systems), Depuis son lancement en 1996, la technologie Flash est devenue une des méthodes les plus populaires pour ajouter des animations et des objets interactifs à une page web ; de nombreux logiciels de création et OS sont capables de créer ou d'afficher du Flash. Flash est généralement utilisé pour créer des animations, des publicités ou des jeux vidéo. Il permet aussi d'intégrer de la vidéo en streaming dans une page, jusqu'au développement d'applications Rich Media.

— d'envoyer et de recevoir le contenu de son choix ;

— d'utiliser les services et les applications de son choix ;

— et de bénéficier d'un haut niveau de concurrence, sur tous les maillons de la chaîne de valeur : accès, terminaux, applications, contenus et services.

Se pose aujourd'hui la question de savoir si le cadre législatif existant, qui sera complété par les dispositions issues de la transposition du paquet télécoms, permet de garantir ces droits ou si ce cadre doit être complété dès à présent.

Le 13 janvier 2011, lors de l'examen en séance du projet de loi portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques, Mme Laure de La Raudière avait déposé un amendement tendant à consacrer le principe de neutralité de l'Internet. Elle l'a retiré après que le ministre de l'Industrie, M. Éric Besson, a souligné que « *le paquet télécoms prévoyait d'ores et déjà une série de mesures de nature à assurer la neutralité d'Internet* » et au profit d'un engagement de ce dernier de poursuivre la réflexion et le débat avec la préoccupation de ne pas compromettre l'économie du secteur.

Le 17 février 2011, l'Assemblée nationale a examiné la proposition de loi n° 3061 sur la neutralité de l'Internet, initiée par M. Christian Paul et déposée par le groupe socialiste. Cette proposition de loi a également été rejetée par l'Assemblée nationale le 1er mars 2011, le ministre de l'Industrie, M. Éric Besson, ayant indiqué que la question de la neutralité du net serait examinée fin novembre 2011 lors des « Assises du numérique », une fois que la Commission européenne et la mission d'information de la commission des affaires économiques sur le sujet auraient achevé leurs travaux.

1. La réglementation des communications électroniques et le droit de la concurrence fournissent d'ores et déjà des garanties importantes pour la préservation d'un Internet ouvert

Comme le rappellent tant le rapport précité du Gouvernement sur la neutralité du net que le rapport (1) de la mission d'information mise en place par la commission des Affaires économiques de l'Assemblée nationale sur la neutralité de l'Internet et des réseaux rendu le 13 avril 2011 par Mmes Corinne Erhel, Présidente, et Laure de La Raudière, rapporteure, outre la liberté de communication reconnue par l'article 10 de la Déclaration des droits de l'homme et du citoyen, la réglementation des communications électroniques comporte déjà plusieurs dispositions permettant de faire face aux risques.

(1) Rapport d'information n° 3336 déposé par la commission des Affaires économiques sur la neutralité de l'Internet et des réseaux et présenté par Mme Corinne Erhel, Présidente, et Mme Laure de la Raudière, rapporteure.

Le droit des communications électroniques prend largement en compte l'objectif de liberté d'accès aux réseaux ainsi que celui de neutralité des opérateurs. L'article L. 32-1 du code des postes et des communications électroniques (CPCE) prévoit ainsi que : « *Dans le cadre de leurs attributions respectives, le ministre chargé des communications électroniques et l'Autorité de régulation des communications électroniques et des postes prennent, dans les conditions objectives et transparentes, des mesures raisonnables et proportionnées aux objectifs poursuivis et veillent : [...]*

— 4° À la définition de conditions d'accès aux réseaux ouverts au public et d'interconnexion de ces réseaux qui garantissent la possibilité pour tous les utilisateurs de communiquer librement et l'égalité des conditions de la concurrence ;

— 5° Au respect par les opérateurs de communications électroniques du secret des correspondances et du principe de neutralité au regard du contenu des messages transmis, ainsi que de la protection des données à caractère personnel ; [...]

— 9° À l'absence de discrimination, dans des circonstances analogues, dans le traitement des opérateurs ; [...]

— 12° À un niveau élevé de protection des consommateurs, grâce notamment à la fourniture d'informations claires, notamment par la transparence des tarifs et des conditions d'utilisation des services de communications électroniques accessibles au public. »

L'obligation de neutralité des opérateurs est déclinée aux articles L. 33-1 et D. 98-5 du CPCE qui dispose que « *L'opérateur prend les mesures nécessaires pour garantir la neutralité de ses services vis-à-vis du contenu des messages transmis sur son réseau et le secret des correspondances. À cet effet, l'opérateur assure ses services sans discrimination quelle que soit la nature des messages transmis et prend les dispositions utiles pour assurer l'intégrité des messages.* » Comme le souligne le rapport précité de Mmes Laure de La Raudière et Corinne Ehrel, ces règles interdisent aux opérateurs de modifier le contenu des informations transportées et non de faire varier les caractéristiques de l'acheminement.

L'article L. 34-8 du CPCE prévoit une obligation générale d'interconnexion pour l'ensemble des exploitants de réseaux ouverts au public et permet à l'ARCEP d'« *imposer, de manière objective, transparente, non discriminatoire et proportionnée, les modalités de l'accès ou de l'interconnexion [...]* », soit de sa propre initiative, soit dans le cadre du règlement d'un litige.

L'article L. 34-8 du même code permet également à l'ARCEP d'imposer certaines obligations aux opérateurs qui contrôlent l'accès à l'utilisateur final, ce qui couvre en particulier les opérateurs d'accès à l'Internet fixe et mobile.

Selon le rapport précité de la mission d'information de la commission des Affaires économiques, « *le pouvoir de règlement des différends de l'ARCEP, prévu par l'article L. 36-8 du CPCE pourrait s'avérer utile. Il est toutefois difficilement utilisable par les petits acteurs, qui doivent faire la preuve d'un traitement inéquitable. Il suppose par ailleurs, pour être efficace, une meilleure connaissance du réseau Internet par le régulateur.* »

Selon le rapport du Gouvernement, « *le CPCE fournit surtout le cadre d'une régulation pragmatique dont les fondements et méthodes sont cohérents avec le droit commun de la concurrence (...). À ce titre, l'ARCEP est en mesure d'imposer aux opérateurs qui exercent une influence significative sur un marché du secteur des communications électroniques diverses obligations en matière d'accès ou d'interconnexion (obligation de transparence, obligation de non-discrimination, séparation comptable, obligation de faire droit aux demandes d'accès au réseau ou aux ressources associées, contrôle des prix).* »

Enfin, le droit de la concurrence prohibe les pratiques qui, d'une part, introduisent une différence de traitement injustifiée, et, d'autre part, ont un effet restrictif sur la concurrence. Il s'agit notamment des pratiques discriminatoires s'inscrivant dans le cadre d'un abus de position dominante ou de dépendance économique.

Dans leur rapport précité, Mmes Ehrel et de La Raudière estiment cependant que « *contrairement à une idée souvent avancée, le droit général de la concurrence n'apporte pas toutes les garanties. Il n'apparaît pas opérant dans le cas de la dégradation du* peer-to-peer*, qui soulève des problèmes qui ne sont pas de nature concurrentielle. Dans les autres cas, l'abus de position dominante suppose de prouver l'existence d'un marché sur lequel il y a position dominante, ce qui n'est pas toujours facile, et la prohibition des ententes admet des exceptions pour promouvoir l'innovation.* »

2. Les dispositions issues de la transposition du troisième paquet télécoms apportent des garanties supplémentaires

Le troisième paquet télécoms contient trois séries de dispositions relatives à la neutralité qui doivent venir compléter notre cadre juridique, l'article 17 de la loi n° 2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques autorisant le Gouvernement à prendre par voie d'ordonnance dans un délai de six mois à compter de la promulgation de la loi les dispositions législatives nécessaires à leur transposition :

– la consécration du principe de neutralité comme objectif de la régulation, à la fois dans sa dimension économique (promotion d'une concurrence effective entre fournisseurs d'accès à Internet et fournisseurs de contenus au bénéfice du consommateur « *y compris pour la transmission de contenu* ») et dans sa dimension sociétale (objectif de « *favoriser l'accès des utilisateurs finaux à*

l'information et préserver leur capacité à diffuser ainsi qu'à utiliser les applications de leur choix ») ;

– des obligations de transparence imposées aux opérateurs en matière de gestion de trafic et de restrictions à l'accès au réseau, pour assurer la protection du principe de neutralité par le jeu de la concurrence (nouvelles mentions obligatoires dans les contrats de services de communications électroniques, devant figurer sous une forme claire, détaillée et aisément accessible : procédures de gestion de trafic, restrictions à l'accès à des services ou à des équipements, réactions pour assurer la sécurité et l'intégrité du réseau, etc.) ;

– l'attribution de nouveaux pouvoirs au régulateur afin de lui permettre d'empêcher la violation du principe de neutralité (pouvoir de fixer des exigences minimales en termes de qualité de service ; pouvoir de règlement des différends étendu aux litiges portant sur l'acheminement du trafic entre des opérateurs et d'autres entreprises, y compris des fournisseurs de contenu).

3. Le débat sur la nécessité de renforcer dès à présent ce cadre législatif

Le rapport gouvernemental sur la neutralité du Net, remis au Parlement début juillet 2010, propose plusieurs pistes d'évolution réglementaire :

— imposer une transparence accrue vis-à-vis des utilisateurs finaux. Si le nouveau cadre communautaire renforce les obligations des opérateurs en la matière, une information effective des consommateurs implique, selon le Gouvernement, de compléter ces obligations par des dispositifs permettant un accès facile aux informations. Le Gouvernement demandera donc aux acteurs concernés de définir un code de bonnes pratiques visant notamment à préciser la mise en œuvre des dispositions du « paquet télécoms » en matière de transparence ;

— fournir aux consommateurs un mécanisme de règlement des litiges avec leur opérateur relatif à la neutralité du net et imposer aux opérateurs de se doter d'un médiateur indépendant chargé de régler ces litiges ;

— introduire un objectif de non-discrimination dans les relations opérateurs-fournisseurs de services pour l'acheminement du trafic ;

— demander à l'ARCEP de définir des lignes directrices encadrant les mécanismes et pratiques de gestion du trafic acceptables de la part des opérateurs.

Fin septembre 2010, l'ARCEP a justement remis un rapport [1] sur la neutralité du net, dans lequel elle :

— pose le principe de l'absence de blocage et de discrimination : l'Autorité recommande aux opérateurs et fournisseurs de services de ne pas différencier les modalités de traitement des flux de données en fonction du type de contenu, de service, d'application, de terminal ou en fonction de l'adresse d'émission ou de réception ;

— ouvre la porte à des exceptions liées aux nécessités de la gestion des flux, dont elle renvoie la définition à des travaux entre différents acteurs concernés et autorise le développement des services gérés à condition que soit garantie la qualité de l'Internet pour éviter que le développement de ces services ne lui nuise ;

— entend soumettre ces exceptions à des critères d'efficacité, de pertinence, de proportionnalité, de transparence et de non-discrimination.

Au-delà, le rapport gouvernemental estime, pour sa part, que l'État doit garantir, sur le long terme, les conditions de développement d'un Internet ouvert, ce qui passe par :

— *la promotion d'une concurrence dynamique sur le marché de l'accès et plus largement sur les différents marchés concernés.*

Si, contrairement à plusieurs interlocuteurs rencontrés à Washington, les rapporteurs ne pensent pas qu'elle soit la pierre philosophale pour résoudre la question de la neutralité de l'Internet, elle constitue incontestablement un levier essentiel pour garantir le maintien d'un Internet ouvert. Sous l'effet de la concurrence et de la demande des utilisateurs, les opérateurs sont encouragés à ne pas discriminer les contenus et à ouvrir l'accès aux services avant leurs concurrents. Sur ce point, la situation concurrentielle apparaît beaucoup plus favorable en France et, plus généralement, en Europe qu'aux États-Unis. De nombreuses mesures ont été prises ces dernières années pour dynamiser la concurrence entre les opérateurs d'accès et faciliter le changement d'opérateur : réduction des délais de portabilité, limitation des durées minimales d'engagement, attribution d'une quatrième licence mobile, etc. Ces efforts doivent être poursuivis.

— *une amélioration de la connaissance des différents marchés de l'Internet afin de pouvoir agir le cas échéant en cas de déséquilibre et besoins de régulation avérés*. Le Gouvernement estime que s'il n'y a pas aujourd'hui de problème majeur, il convient de rester vigilant compte tenu de la rapidité d'évolution du secteur de l'Internet. Un suivi et une connaissance accrue du fonctionnement du marché de gros de l'interconnexion de données, aujourd'hui très mal connu, apparaissent en particulier prioritaires. C'est pourquoi le

(1) Neutralité de l'Internet et des réseaux: propositions et recommandations, *ARCEP, septembre 2010.*

Gouvernement a demandé à l'ARCEP de développer un suivi de ce marché et d'améliorer la connaissance de sa situation concurrentielle ;

— *l'accroissement des capacités de réseaux disponibles*. L'investissement dans de nouvelles infrastructures et notamment l'augmentation de la capacité des réseaux mobiles et le développement de la fibre optique sont probablement la seule réponse efficace à l'augmentation du trafic à moyen et long terme mais ils soulèvent la question de leur financement.

La mission d'information de la commission des Affaires économiques estime au contraire que le cadre juridique de la neutralité du net doit être complété dès à présent. Elle juge qu'« *il n'existe pas de réelle contrainte constitutionnelle ou de droit européen ; le cadre juridique est dans son ensemble relativement peu contraignant pour les opérateurs ; le contenu des règles en vigueur est incertain car elles procèdent pour l'essentiel, soit de la régulation sectorielle ou concurrentielle générale, sans que les applications existent à l'heure actuelle, soit de pouvoirs nouveaux issus du troisième paquet télécoms, qui ne sont pas encore entrés en vigueur.* »

Estimant qu'il existe aujourd'hui *un risque* que se développent des pratiques non neutres qui réduiraient la capacité des utilisateurs d'Internet à choisir l'usage qu'ils font du réseau, elle propose, pour faire face à ce risque, de donner une portée juridique au principe de neutralité de l'Internet, en fixant de manière générale sa promotion comme objectif aux autorités. Le principe de neutralité serait défini dans la loi comme « *la capacité pour les utilisateurs d'Internet :*

— *d'envoyer et de recevoir le contenu de leur choix ;*

— *d'utiliser les services ou de faire fonctionner les applications de leur choix ;*

— *de connecter le matériel et d'utiliser les programmes de leur choix, dès lors qu'ils ne nuisent pas au réseau, avec une qualité de service transparente, suffisante et non discriminatoire, et sous réserve des obligations prononcées à l'issue d'une procédure judiciaire et des mesures nécessitées par des raisons de sécurité et par des situations de congestion non prévisibles.* »

Pour éclairer le choix du consommateur, la mission d'information de la commission des Affaires économiques propose de réserver l'appellation Internet aux seuls accès neutres et d'instituer, au sein de l'ARCEP, un observatoire de la qualité de l'Internet.

Dans l'hypothèse où la concurrence ne permettrait pas au consommateur d'opter pour un accès à Internet neutre de qualité à un prix raisonnable, la mission d'information de la commission des Affaires économiques souhaite que la capacité de choix du consommateur puisse être rétablie par des moyens plus

contraignants consistant à imposer aux fournisseurs d'accès à Internet des exigences garantissant la qualité d'Internet édictées par l'ARCEP.

Enfin, afin d'assurer le financement pérenne de l'Internet, la mission d'information de la commission des Affaires économiques estime que si les fournisseurs d'accès à Internet sont obligés de fournir un Internet de qualité suffisante, il convient de s'assurer que leur modèle économique leur permette de le faire. L'institution d'une « terminaison d'appel data » constituerait à cet égard, selon la mission, une piste intéressante. Il s'agirait de mettre en place « *un mécanisme par lequel les opérateurs induisant le trafic paieraient aux fournisseurs d'accès à Internet un montant dépendant de la partie asymétrique du trafic échangé et permettant de couvrir les coûts incrémentaux supportés par les fournisseurs d'accès à Internet du fait de la hausse du trafic* », c'est-à-dire un mécanisme permettant d'assurer une meilleure répartition des coûts liés à l'accroissement du trafic sur le réseau entre les fournisseurs de services et les fournisseurs d'accès à Internet. La mission d'information de la commission des Affaires économiques admet cependant que cette proposition soulève de nombreuses interrogations techniques et juridiques. Il s'agit donc d'une piste à approfondir au niveau européen, la mise en place d'une terminaison d'appel data au seul niveau français ne paraissant pas opportune.

Au contraire, dans son rapport de juillet 2010, le Gouvernement estime qu'« *il n'est pas apparu dans les dernières années de problèmes majeurs ou répétés en matière d'atteinte à la neutralité de l'Internet* » et que « *la réflexion sur la nécessité ultérieure de nouvelles évolutions législatives pourrait continuer, en fonction de l'évolution des marchés et à la lumière des travaux au niveau communautaire et national qui vont se poursuivre dans les prochains mois.* »

La Commission européenne vient en effet de remettre un Livre blanc sur le sujet, dans lequel elle estime qu'il n'est pas souhaitable, à ce stade, de renforcer la réglementation en matière de neutralité de l'Internet.

Le rapport de la Commissaire européenne, Mme Neelies Kroes, se contente d'observations, et ne propose à ce stade aucune mesure supplémentaire pour garantir le respect du principe de neutralité.

Pour la Commission européenne, une intervention du régulateur européen apparaît prématurée dans la mesure où les États membres sont encore engagés dans la transposition de la directive sur les communications électroniques - qui devra s'achever le 25 mai 2011. La Commission préconise d'attendre de pouvoir mesurer les impacts des règles fixées par ladite directive.

Le rapport de Mme Kroes juge par ailleurs les données recueillies durant la consultation publique incomplètes et imprécises sur de nombreux aspects, et notamment sur l'existence de pratiques abusives des opérateurs. L'autorité européenne estime donc indispensable d'approfondir au préalable la réflexion sur différents aspects de la neutralité : les barrières au changement d'opérateur, les

pratiques de filtrage et commerciales ou encore la transparence et la qualité de service.

Les risques de blocage ou de dégradation de services par les opérateurs, au profit par exemple de leurs propres offres, sont relativisés par la Commission. Selon elle, aucune preuve n'atteste de l'existence de telles pratiques à ce stade.

M[e] Winston Maxwell, avocat à la cour d'appel de Paris, auditionné le 10 novembre 2010, a estimé qu'une vision égalitaire d'Internet, où il n'y aurait ni riches ni pauvres, est une fiction. Néanmoins, il serait selon lui prématuré de dire que la neutralité du Net est violée. L'organisme qui fédère l'ensemble des organismes de régulation européens *(BEREC* [(1)]*)* a d'ailleurs reconnu, dans un rapport publié le 8 octobre 2010, que très peu de problèmes étaient relevés sur le terrain. Les quelques cas connus ont été résolus très vite sans l'intervention d'un régulateur. La prudence s'impose donc avant d'affirmer que le système actuel ne fonctionne plus.

Tout bien considéré, la question qui se pose aujourd'hui, s'agissant de la neutralité de l'Internet, est, comme aux États-Unis, celle de la légitimité d'une intervention du législateur et d'un renforcement de la régulation pour faire face à des risques ou si cette intervention n'est légitime que si une « défaillance du marché » est réellement avérée et constatée.

Sur cette question délicate qui est aujourd'hui en débat comme on vient de le montrer, vos rapporteurs portent un regard différent.

M. Patrick Bloche, rapporteur, cosignataire de la proposition de loi n° 3061 sur la neutralité de l'Internet, estime comme il a pu l'exprimer lors de l'examen en séance de ce texte, le 17 février 2011, que l'inscription dans la loi de ce principe de neutralité constituerait une garantie contre les menaces pouvant peser sur un Internet libre et ouvert. C'est pourquoi il est favorable à l'inscription de ce principe dans la loi sans plus attendre.

M. Patrice Verchère, rapporteur, juge, pour sa part, que la question de la neutralité du Net se pose à l'évidence mais que la réflexion doit être poursuivie quant à l'intérêt de proclamer ainsi dans la loi un principe dont les modalités de mise en œuvre resteraient largement à déterminer. Il estime nécessaire que soit menée une étude sur l'efficacité des mesures récemment adoptées avec la transposition du paquet télécoms ainsi que sur les cas d'atteinte avérée à la neutralité du Net.

B. ENCADRER LE BLOCAGE ET LE FILTRAGE LÉGAUX ?

Rappelons que la notion de neutralité du net renvoie à l'idée que toutes les données sont transportées et traitées de la même manière, de leur point d'origine jusqu'à leur destination finale. Elle serait ainsi remise en cause par toutes les

(1) BEREC *:* Body of European Regulators of Electronic Communications.

pratiques de dégradation ou de ralentissement du trafic par les opérateurs mais aussi par les pratiques de blocage de la transmission de données décidées par le législateur.

1. Les arguments en faveur du blocage légal

À l'occasion du débat sur la LOPPSI, les partisans du blocage ont fait valoir, en faveur du dispositif de blocage proposé, que des dispositifs de ce type avaient été mis en œuvre à l'étranger avec succès, que le blocage représentait une restriction de la liberté d'expression qui n'était pas excessive (étant notamment contestable devant le juge) et avait d'ailleurs été validée par le Conseil constitutionnel et qu'une procédure passant par l'autorité administrative, plutôt que le juge, permettait une plus grande réactivité.

Lors de la table ronde organisée par la mission le 9 novembre 2010, les représentants d'associations de protection de l'enfance sur Internet ont défendu la mise en place d'un blocage de l'accès aux sites pédopornographiques. Mme Justine Atlan, directrice de l'Association e-enfance, a estimé qu'une loi sur le filtrage des sites pédopornographiques était manifestement nécessaire, les fournisseurs d'accès à Internet ne s'impliquant, à son avis, pas suffisamment sur cette question. La pédopornographie étant un contenu de nature illégale, l'exigence de filtrer des contenus illégaux ne devrait, selon elle, pas poser le moindre problème.

Mme Véronique Fima-Fromager, directrice d'Action innocence, a estimé que le sujet de la lutte contre les contenus pédopornographiques avait été transformé en question de principe, de nombreux détracteurs en ayant appelé à la liberté d'expression. S'agissant cependant de contenus illicites, elle a considéré qu'il n'y avait pas débat. S'agissant des modalités de mise en place d'un système de filtrage, elle a rappelé que d'autres pays tels que la Norvège, le Royaume-Uni ou la Suède y étaient très bien parvenus, la France étant tout aussi capable d'appliquer de telles mesures techniques.

En revanche, les associations ont rappelé leur attachement à une intervention préalable de l'autorité judiciaire. M. Dominique Delorme, responsable de la ligne Net Écoute de l'Association e-enfance, a souligné que l'ensemble des participants aux travaux du Forum des droits de l'Internet sur ce sujet avaient envisagé la création d'une commission permanente chargée de juger du caractère pédopornographique des sites, avec une mise à jour biquotidienne des listes transmises aux fournisseurs d'accès, et avaient insisté sur le fait que le juge devait être présent au sein de cette commission de façon à pouvoir être saisi immédiatement.

2. Les arguments contre le blocage légal

Dans un ouvrage consacré à la neutralité d'Internet, MM. Nicolas Curien et Winston Maxwell observent à juste titre que, « *s'il existait un moyen technique*

permettant, avec une précision chirurgicale, de bloquer uniquement les contenus illégaux, sans affecter les contenus légaux ni risquer d'enfreindre aucun droit fondamental, sans doute le débat serait-il plus simple et plus serein ! » (1)

Cette observation montre que le débat est beaucoup plus technique et beaucoup moins idéologique qu'il n'en a l'air.

La mission d'information de la commission des Affaires économiques a souligné les nombreux défauts des mesures de blocage :

— les techniques de contournement des mesures de filtrage sont relativement accessibles. Dans les cas où le blocage vise des échanges de contenu réellement odieux, comme des images pédopornographiques, les pouvoirs publics font face à des groupes criminels organisés qui utilisent Internet de manière sophistiquée et réussiront à échapper aux obligations de blocage. Le simple blocage d'un site web est difficile. Il existe en outre, selon les rapporteures, Mmes Ehrel et La Raudière, un risque global lié au développement de techniques de contournement des mesures de blocage. Dans les cas où le blocage vise des échanges « grand public », comme des jeux en ligne, il peut être dissuasif à court terme. À long terme, cependant, il ne faut pas sous-estimer la capacité des internautes à utiliser massivement des techniques de contournement. Une telle évolution serait une menace pour la sécurité du réseau et constituerait de surcroît un grave problème dans les relations entre le monde virtuel de l'Internet et les pouvoirs publics. Elle suscite d'ailleurs, selon la mission précitée, l'inquiétude des forces de cybersécurité ;

— à l'inefficacité partielle des mesures de blocage s'ajoutent, selon la mission d'information de la commission des Affaires culturelles, des risques de « surefficacité », les techniques disponibles engendrant des « surblocages » (blocage de contenus, services ou application légaux, autres que ceux visés).

Notre mission a également entendu de nombreux arguments qui incitent à s'interroger sur la pertinence et l'efficacité des mesures de blocage.

Lors de la réunion de travail organisée par la mission le 19 janvier 2011 M. Thomas Jarzombek, député du *Bundestag*, président des groupes de travail sur la protection des mineurs et l'éducation des médias au sein de la commission numérique a souligné que la question du blocage légal était également débattue en Allemagne. Il a précisé que la loi existante, qui le permet, n'était pas appliquée car des doutes demeurent, comme en France, sur la compatibilité d'une telle mesure avec les droits fondamentaux.

L'Association des fournisseurs d'accès et de services Internet (AFA) est évidemment très opposée aux mesures de blocages. Dans un communiqué du 3 mars 2010, l'AFA estime qu'« *il est toujours plus efficace d'agir à la source même du contenu, en le faisant retirer par l'hébergeur du site Internet, plutôt que*

(1) Nicolas Curien et Winston Maxwell, La neutralité d'Internet, *La Découverte, 2011, p. 69.*

de le faire bloquer par les FAI français. Lorsqu'un contenu est bloqué, il reste en ligne, et n'est que temporairement inaccessible puisque la mesure de blocage est facilement contournable. » L'auteur du contenu bloqué peut en effet en quelques minutes faire héberger son site sous un autre nom de domaine ou une autre URL, selon la technique de blocage utilisée.

Quant à l'internaute souhaitant accéder au site qui fait l'objet du blocage, il dispose, selon l'AFA de plusieurs outils de contournement. « *Il peut notamment demander l'accès au site de façon anonyme, par l'intermédiaire d'un « anonymiseur », qui lui permettra d'utiliser un DNS (1) non sujet à restrictions. L'internaute peut encore utiliser le DNS d'un FAI étranger, en modifiant l'un des paramètres de sa connexion Internet. Enfin, le blocage n'empêchera pas la diffusion de contenus de pornographie enfantine, très nombreux, via les réseaux* peer-to-peer. »

M. Édouard Barreiro, chargé de mission nouvelles technologies à l'UFC « Que choisir ? », entendu par la mission le 3 novembre 2010, a expliqué que la loi sur la confiance dans l'économie numérique fournissait déjà aujourd'hui de très bons outils permettant de lutter contre les contenus illégaux, en ouvrant la possibilité de s'adresser à la personne qui a fourni le contenu litigieux, de remonter à l'hébergeur du site, et éventuellement jusqu'à l'opérateur. Il a considéré que le filtrage était insuffisant en ce qu'il ne permettait pas de supprimer le contenu des sites, mais seulement de faire croire qu'il n'existait plus.

Le système du retrait à la source a pris une dimension concrète en 1998 avec la mise en place du service de signalement de contenus choquants « Point de Contact ». Une Charte sur les « contenus odieux » a par ailleurs été signée le 14 juin 2004 par l'AFA et ses membres. La LCEN a mis à la charge des FAI et hébergeurs une obligation de signaler aux autorités compétentes plusieurs types de contenus illégaux qui leur seraient signalés. La hotline « Pointdecontact.net » est ainsi devenue le relais de l'obligation légale de signalement des membres de l'AFA : tout contenu potentiellement illégal selon l'article 6 de la LCEN reçu par « Point de Contact » est transféré aux autorités compétentes (l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication), à l'hébergeur du contenu si ce dernier est membre de l'AFA, ou à un partenaire du réseau *Inhope*, fédération internationale de services d'assistance en ligne (*hotlines*) luttant contre les contenus odieux, selon le pays d'hébergement du contenu, afin d'être retiré.

Une mesure de blocage par l'autorité judiciaire peut par ailleurs avoir des conséquences contraires à l'objectif visé, comme cela a été le cas pour le site négationniste « Aaargh », hébergé aux États-Unis et auquel la Cour de cassation a obligé en 2008 les fournisseurs français à empêcher l'accès. La décision de bloquer ce site en France a contribué à la diffusion de son contenu, et la publicité

(1) Le Domain Name System *(ou DNS, système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.*

faite autour de l'affaire a largement participé à la notoriété d'un site au départ confidentiel. Son contenu s'est retrouvé dupliqué très rapidement sur de nombreux sites miroirs, échappant de cette manière aux mesures de blocage mises en place.

M. Fabrice Le Fessant, chargé d'enseignement à l'École polytechnique, auditionné le 5 mai 2010, a expliqué qu'un logiciel comme *Skype* permettait de procéder à des transferts de données selon un protocole chiffré. Dans ce cas, aucune solution de filtrage n'existe car il est impossible de distinguer la communication téléphonique du transfert de fichier. Si le filtrage devait se développer, M. Le Fessant a estimé que les concepteurs de logiciels s'orienteraient probablement vers des solutions inspirées de la technologie *Skype*. De façon générale, il a mis en garde contre le fait que le filtrage pousse au chiffrage et conduit à une situation qui rend les contrôles légitimes beaucoup plus difficiles. Le filtrage est selon lui « *une fausse bonne solution* » et « *une technologie qui ne fonctionnera pas* ».

Au cours de la même audition, M. Thomas Clausen, maître de conférences à l'École polytechnique, a précisé qu'il existait aussi des réseaux qui ne passaient pas par des fournisseurs d'accès et qui ne pouvaient en conséquence pas être l'objet de blocages. Ce type de réseaux, dont les protocoles ont été établis depuis longtemps, a été utilisé en situation d'urgence, par exemple à Haïti, pour permettre aux médecins et aux pompiers de communiquer. Mais surtout il existe de grands réseaux communautaires développés selon ce principe, par exemple à Berlin, à Seattle, à Leipzig et à Lille. Pour le moment ce sont surtout des initiatives mises en place par des étudiants ou des universitaires, mais on peut imaginer d'autres usages. Leur nombre a fortement augmenté, il augmentera encore si le réseau ouvert fait l'objet d'un filtrage croissant. Pour s'opposer à un filtrage, on peut en effet soit chiffrer tout un trafic, soit fabriquer un réseau.

3. La position de la mission

Compte tenu des nombreuses réserves et des arguments très forts qu'elle a entendus au cours de ses travaux contre les mesures de blocage, la mission estime que les conclusions de la mission mise en place par la commission des Affaires économiques sur ce sujet méritent une attention toute particulière.

Le rapport de la mission d'information de la commission des Affaires économiques propose d'éviter au maximum d'obliger les opérateurs à bloquer des communications électroniques compte tenu de ce que « *le blocage a des effets négatifs directs (restriction de la liberté d'expression et de communication) et indirects (surblocage, développement du chiffrement, etc.)* ». La rapporteure de cette mission d'information regrette que ces effets négatifs ne soient pas toujours correctement pris en compte dans les décisions législatives.

De plus, cette mission souligne, à très juste titre, que l'éclatement des bases législatives (principe de subsidiarité posé par l'article 6 de la LCEN de 2004, remise en cause de ce principe par la loi précitée sur les jeux en ligne de

2010 et la LOPPSI) est un facteur de confusion. C'est pourquoi, elle propose de « *s'interroger plus avant sur la justification des mesures de blocage légales, en dépit de leur légitimité apparente, du fait de leur inefficacité et des effets pervers qu'elles sont susceptibles d'engendrer et de prévoir dès à présent l'intervention systématique du juge pour prononcer des mesures obligatoires de blocage afin de mieux protéger la liberté d'expression.* »

Mmes Ehrel et La Raudière se demandent si les bénéfices attendus de la mise en œuvre de mesures obligatoires de filtrage ne sont pas inférieurs aux risques engendrés et, lorsque c'est le cas, s'il n'est pas préférable de s'abstenir d'introduire de nouvelles bases légales donnant au juge le pouvoir de prononcer des mesures obligatoires de blocage.

Orientation n° 42 : Une évaluation des mesures de blocage légal

Notre mission estime :

– que l'ensemble des éléments qui a été porté à sa connaissance justifie *a minima* qu'il soit procédé à une évaluation des mesures de blocage légal – aucun nouveau cas de filtrage n'étant ajouté aux cas existants en attendant ;

– et que l'intervention du juge doit être prévue dans tous les cas de blocage légal.

C. ÉLARGIR LA RÉFLEXION SUR LA NEUTRALITÉ DE L'INTERNET AUX AUTRES ACTEURS

À quoi bon des infrastructures neutres si les terminaux d'accès filtrent l'accès aux contenus et aux plateformes qui sont sur ce réseau ? À quoi bon disposer de milliards d'informations potentielles si l'on ne peut y accéder parce que les instruments de recherche nous guident systématiquement vers des contenus priorisés, d'intérêt commercial ? Voici quelques-unes des questions qu'il nous faut nous poser si nous souhaitons garantir sur le long terme un Internet libre et ouvert. C'est pourquoi il faut élargir la réflexion sur la neutralité des réseaux à celle de la neutralité des terminaux et celle du référencement.

1. Quelle neutralité des moteurs de recherche ?

Le rôle central des moteurs de recherche comme principale voie d'accès aux contenus mis en ligne conduit à examiner la nature de leurs critères de classement. Les outils d'indexation des pages Web traçant les chemins d'accès au savoir et à la connaissance ne sont pas neutres. Ainsi, avec leurs propres algorithmes, les moteurs de recherche imposent leurs règles de hiérarchisation des contenus.

Plus des deux tiers des requêtes sur le Web passent par un seul moteur de recherche, donnant accès à quelque 30 milliards de pages indexées et classées en fonction de plus de 200 paramètres, dont le « *PageRank* » qui mesure la popularité d'un site à la qualité et à la quantité des liens pointant vers celui-ci. De cette façon,

Google investit toutes les sources d'audience possibles afin d'engendrer le maximum de trafic sur le Web et de vendre des mots-clés ou des liens sponsorisés qui lui assurent 98 % de ses revenus.

Selon M. Marc Mossé, directeur des affaires publiques et juridiques de la société *Microsoft France*, auditionné par la mission le 29 septembre 2010, le principe de neutralité s'applique aussi aux critères selon lesquels se font les recherches sur Internet. Ceux-ci doivent selon lui être objectifs et rationnels. Sans qu'il faille rendre publics les algorithmes utilisés par chaque moteur de recherche, il a estimé qu'il conviendrait de faire en sorte que l'utilisateur conserve toute sa confiance envers les outils utilisés. Cette exigence est d'autant plus forte que les moteurs de recherche deviendront peut-être les principaux points d'accès à l'information et à la culture. L'expérience montre, en outre, que les internautes dépassent rarement la deuxième page des résultats affichés lors d'une recherche. Ainsi des sites peuvent-ils être artificiellement rétrogradés sur les pages suivantes ce qui signifie qu'ils ne sont pas consultés. Selon M. Marc Mossé, certains acteurs du Net peuvent proposer des moteurs de recherche plus « verticaux » qui favorisent certains résultats.

La meilleure solution pour améliorer la qualité et l'objectivité du référencement des moteurs de recherche serait un accroissement de la concurrence sur ce marché.

M. Stéphane Richard, directeur général de France Télécom/Orange, lors de son audition du 22 juin 2010, a relevé que, lorsque vous effectuez une recherche sur la neutralité du net sur *Google*, qui est l'un des plus ardents défenseurs de ce principe, ce dernier vous emmène en priorité sur quatre sites qui défendent ses propres positions sur la question. « *N'y a-t-il pas là une atteinte à la neutralité du net* ? », s'est-il interrogé.

Mme Meryem Marzouki, présidente de l'association IRIS *« Imaginons un réseau Internet solidaire »*, lors d'une table ronde organisée par la mission de 25 mai 2010, a jugé que les modes d'utilisation par défaut de certains services sur l'Internet gagneraient aussi à être précisés : il conviendrait par exemple que *Google* permette de procéder à des recherches sans qu'il soit tenu compte de l'historique des précédentes requêtes.

En réponse à l'ensemble de ces critiques, M. Yoram Elkaïm, directeur juridique « *Southern and Eastern Europe, Middle East and Africa* » de la société *Google*, a rappelé, lors de l'audition du 8 septembre 2010, que l'utilisation d'un moteur de recherche n'était soumise à aucune obligation d'abonnement. L'internaute conserve dès lors la possibilité de recourir à tout moment aux services d'un moteur de recherche concurrent. Ce risque économique s'oppose, selon lui, à ce que l'utilisation d'un moteur de recherche aboutisse à des classements arbitraires. Certes, chaque moteur de recherche choisit de manière subjective sa technologie de classement mais son application doit se faire de manière homogène et objective sur l'ensemble des contenus référencés. En ce

sens, l'algorithme de classement constitue un véritable savoir-faire propre à la société *Google* qui garantit la pertinence des résultats et justifie la confiance que les internautes lui accordent.

Comme le souligne le rapport gouvernemental sur la neutralité de l'Internet, des interrogations se font donc jour :

— d'une part, sur le caractère objectif de la présentation des résultats par le moteur : *Google* a ainsi fait l'objet de plaintes en février 2010 auprès de la Commission européenne de la part de deux entreprises : Foundem (comparateur de prix britannique) et eJustice.fr (moteur de recherche spécialisé dans le droit). Si les termes des plaintes ne sont pas connus, ils porteraient selon *Google* sur le fait que les algorithmes du moteur pénaliseraient ces acteurs dans l'affichage des résultats, car étant considérés comme des moteurs verticaux concurrents. Récemment, l'Autorité de la concurrence saisie par la société NAVX (société qui commercialise des avertisseurs de radars principalement sur Internet et notamment *via* la régie publicitaire Adwords) a prononcé des mesures d'urgence à l'encontre de *Google*, estimant que la politique de contenus du service AdWords avait été mise en œuvre par *Google* dans des conditions qui manquaient d'objectivité et de transparence et qui conduisaient à traiter de façon discriminatoire les fournisseurs de base de données radars ;

— d'autre part, sur des accords d'exclusivité portant sur l'indexation de certains contenus : cette problématique a notamment été soulignée pour le livre numérique dans le rapport sur la numérisation du patrimoine écrit remis par M. Marc Tessier au ministre de la Culture et de la communication et à la secrétaire d'État chargée de la prospective et du développement de l'économie numérique en janvier 2010. Le rapport notait que « *les accords passés par Google prévoient toujours que les autres moteurs de recherche ne pourront pas accéder aux fichiers numérisés par lui pour les indexer et les référencer* » et recommandait de refuser catégoriquement toute mesure technique interdisant l'indexation du texte par les moteurs de recherche.

Naturellement, les résultats présentés par un moteur de recherche en réponse à une requête présentent un caractère subjectif ; ils dépendent en effet des critères choisis pour juger de la pertinence d'une page par rapport à une requête. Toutefois, une certaine garantie d'égalité de traitement est supposée (et attendue) de ce type d'outils.

Compte tenu de la complexité et des enjeux, une réflexion approfondie apparaît souhaitable sur ce sujet. Le caractère mondial des principaux moteurs de recherche implique, par ailleurs, que cette réflexion soit menée au plan européen voire international.

Dans cette perspective, le Gouvernement indique, dans le rapport du 16 juillet 2010, qu'il proposera à la Commission européenne d'aborder la question de la neutralité du référencement par les moteurs de recherche dans le

prolongement de la consultation publique sur la neutralité de l'Internet qu'elle a lancée le 30 juin 2010.

2. La neutralité des terminaux

Comme le relève le rapport gouvernemental sur la neutralité de l'Internet, le développement des « smartphones » fait apparaître de nouveaux enjeux en matière de neutralité de l'Internet.

Sur les réseaux mobiles, l'accès à certaines applications (par exemple l'Apple Store sur l'Iphone) peut être favorisé par l'opérateur ou le fabriquant du terminal. Une différenciation de traitement est ainsi mise en place entre différents services. L'accès à certaines applications peut en outre être limité par le fabricant de terminal. Par ailleurs, certains sites web ne sont pas accessibles *via* certains terminaux, pour des raisons qui n'apparaissent pas uniquement d'ordre technique. Par exemple, les Iphones ne prennent pas en charge la technologie *flash* (1).

Ces éléments soulèvent naturellement des questions au regard de l'objectif de neutralité de l'Internet. La *Federal Trade Commission* américaine a d'ailleurs lancé récemment une enquête sur les plateformes d'Apple. L'arrivée de nouveaux systèmes d'exploitation de terminaux mobiles concurrents et plus ouverts par rapport aux applications (avec le système d'exploitation Androïd) est de nature à faire évoluer positivement cette situation.

À ce stade, une vigilance apparaît cependant nécessaire.

Au-delà des terminaux mobiles, de premiers partenariats entre constructeurs de télévision et acteurs de l'audiovisuel (éditeurs, hébergeurs, éventuellement diffuseurs) laissent penser que le sujet de la neutralité des terminaux pourrait se poser également en raison de l'arrivée massive sur le marché des « téléviseurs connectés ».

De nombreux téléviseurs (Samsung, Sony...) permettent d'ores et déjà l'accès, en plus des services de télévision classique, à des services additionnels tels que des services interactifs via des « *widgets* » (2). Ces contenus délivrés par des partenaires du constructeur sont formatés spécifiquement et accessibles uniquement sur le téléviseur de la marque.

Les accords aujourd'hui mis en place entre constructeurs et fournisseurs de contenus audiovisuels prévoient, pour certains d'entre eux, des clauses d'exclusivité, au moins à titre transitoire. Si ces clauses devaient s'étendre sur une

---

(1) Flash Player, développé et distribué par Macromedia (racheté en 2005 par Adobe Systems), Depuis son lancement en 1996, la technologie Flash est devenue une des méthodes les plus populaires pour ajouter des animations et des objets interactifs à une page web ; de nombreux logiciels de création et OS sont capables de créer ou d'afficher du Flash. Flash est généralement utilisé pour créer des animations, des publicités ou des jeux vidéo. Il permet aussi d'intégrer de la vidéo en streaming dans une page, jusqu'au développement d'applications Rich Media.

(2) Widget est une contraction des mots window *et gadget. Un widget interactif est un petit outil qui permet d'obtenir des informations (météo, actualité, dictionnaire, carte routière…).*

durée trop longue, elles pourraient soulever des problèmes concurrentiels et conduire à des modèles fermés, avec le risque d'une concurrence en silo (terminaux et contenus) préjudiciable à l'utilisateur final.

Orientation n° 43 : élargir la notion de neutralité de l'Internet aux autres acteurs du Web

La mission estime qu'une réflexion approfondie est nécessaire sur la neutralité des moteurs de recherche. Le caractère mondial des principaux moteurs de recherche implique que cette réflexion soit menée au plan européen voire international.

Par ailleurs, une réflexion prospective approfondie sur les télévisions connectées doit être lancée afin que soit maintenue l'ouverture des terminaux et des principales plateformes de services.

DEUXIÈME PARTIE : AMÉLIORER L'ÉGALITÉ DANS LES CONDITIONS D'ACCÈS À INTERNET : LA LUTTE CONTRE LES FRACTURES NUMÉRIQUES

L'accès aux réseaux et aux technologies numériques est devenu l'une des conditions d'intégration dans notre société, ainsi que le souligne le plan France numérique 2012. Bien que le Conseil constitutionnel n'y ait pas reconnu de droit créance à l'accès à Internet, dans une vision prospective, sa décision n° 2009-580 DC du 10 juin 2009, rattachant le droit d'accès à une liberté fondamentale, est une incitation de plus à l'extension de l'Internet haut débit pour tous et à la lutte contre la fracture numérique sous toutes ses formes. Internet étant tout à la fois un moyen d'expression, un outil professionnel, un instrument de commerce, un vecteur d'accès à l'information, à la culture, aux services administratifs, une ressource éducative et une voie d'intégration sociale, dans la révolution numérique, le plus grand risque est sans doute de se retrouver « du mauvais côté de la rupture technologique ».

La notion de fracture numérique est née aux États-Unis avec l'émergence d'Internet. Dès le début des années 1990, des études avaient souligné les risques que certains groupes sociaux, essentiellement les plus pauvres, soient exclus de l'accès à Internet et partant de l'accès à l'information et à la vie démocratique et citoyenne. Au cours des années 2000, la notion a évolué pour concerner :

— d'une part, les écarts territoriaux existants entre les zones urbaines bien couvertes par le haut débit et les zones rurales, disposant d'un accès beaucoup plus restreint ;

— et, d'autre part, les écarts entre groupes sociaux, y compris entre les générations.

La fracture numérique repose sur trois types d'inégalités :

— inégalité dans les possibilités d'accès aux réseaux, qui dépendent de la situation géographique et des infrastructures qui y sont accessibles (type de technologie, qualité du débit…) ;

— inégalité dans la capacité à s'équiper à domicile en acquérant un ordinateur et en payant un abonnement ;

— et inégalité dans la maîtrise d'Internet qui suppose de comprendre le fonctionnement des outils et des services et de savoir trouver l'information que l'on recherche tout en étant capable de l'analyser.

Ainsi la lutte contre les fractures numériques est-elle un enjeu d'autant plus crucial pour les pouvoirs publics que la révolution numérique se développe en premier lieu auprès des personnes qui sont déjà les mieux intégrées dans l'économie et la société. La révolution numérique serait donc susceptible, non pas

de résorber, mais d'approfondir les fractures territoriales, sociales et générationnelles.

I. LES FRACTURES NUMÉRIQUES EN FRANCE

A. LE TAUX D'ACCÈS À INTERNET : LA FRANCE EN RETARD

La loi n° 2008-776 du 4 août 2008 de modernisation de l'économie puis la loi n° 2009-1572 du 17 décembre 2009 relative à la lutte contre la fracture numérique ont défini les conditions de déploiement géographique d'un réseau très haut débit sur notre territoire.

Mais permettre l'accès à tous ne suffit pas, si les citoyens ne cherchent pas ou n'ont pas les moyens de s'y raccorder, ou encore s'ils ne disposent pas des capacités d'en exploiter les potentialités. Or, la France est de ce point de vue en retard : en 2010, près de 30 % de la population ne disposait pas d'une connexion à Internet à domicile, tandis que plusieurs pays de l'OCDE s'approchent ou ont parfois dépassé la barre des 90 % de taux d'équipement (Corée du Sud, Islande, Pays-Bas, Suède, Danemark, Norvège).

Cependant cette proportion est en progression quasiment linéaire et a encore gagné 4 points en 2010. En 2009, environ un tiers de la population française ne disposait pas de connexion à Internet. Une étude du CREDOC (Centre de recherche pour l'étude et l'observation des conditions de vie) de décembre 2010 fait le point sur la diffusion des technologies de l'information et de la communication dans la société française en 2010. Elle montre qu'en dix ans, l'évolution est spectaculaire puisque le niveau des inégalités a été divisé par 2,3 pour l'ordinateur et par presque trois pour l'accès à Internet à domicile.

M. Guillaume Buffet, co-président du groupe de réflexion *Renaissance numérique*, au cours de son audition par la mission le 6 juillet 2010 a rappelé qu'en 2007, la France connaissait un retard important dans l'accès à Internet : seuls 45 % des Français étaient connectés contre une moyenne de 80 % en Europe du Nord. *Renaissance numérique* avait alors rédigé un Livre blanc, signé par plus de trente entrepreneurs et chercheurs, qui proposait, en particulier, de créer un ministère de l'Internet, – à savoir une autorité habilitée à coordonner la politique publique en ce domaine – et d'autoriser les entreprises à céder leurs ordinateurs à leurs employés, mesure qui a été adoptée en loi de finances pour 2008.

Aujourd'hui, en 2010, il a estimé que la situation demeurait insatisfaisante : l'engagement pris d'atteindre un niveau de connexion de 80 % de la population française n'a pas été rempli. C'est ce qui constitue, selon *Renaissance numérique*, le plus grand péril pour l'avenir, et non les mauvais usages qui sont faits d'Internet. Il convient, en effet, de dénoncer l'attitude consistant à susciter et à nourrir des peurs envers le Web ; une telle attitude aura pour conséquence de créer des retards dans le développement de ce secteur. Or

Internet est un instrument indispensable, sans lequel on ne peut, aujourd'hui, ni trouver du travail ni créer une entreprise. Rappelant qu'un tiers des Français n'étaient pas connectés au monde numérique, M. Guillaume Buffet a conclu qu'on était, par conséquent, en droit de constater l'existence d'un « tiers net », à l'instar du « tiers-monde » dont parlait Alfred Sauvy.

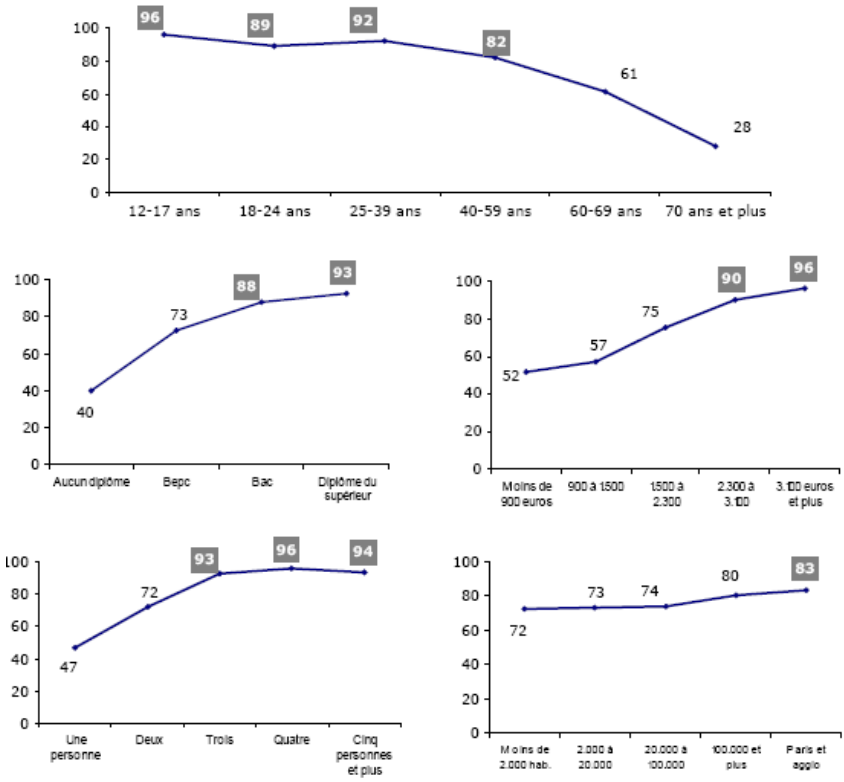
Cette fracture correspond en réalité non pas à un mais à trois fossés numériques, liés à la possession des outils, mais aussi à leur usage : un fossé générationnel, laissant les personnes âgées largement en marge des nouvelles technologies ; un fossé social, qui exclut les plus démunis ; un fossé culturel, qui prive les moins instruits des opportunités du numérique.

B. LES INÉGALITÉS D'ÉQUIPEMENT EN ORDINATEUR À DOMICILE

En dix ans, la part des personnes disposant d'un micro-ordinateur à domicile a plus que doublé : 76 % en 2010, contre 34 % seulement en 2000.

Bien que l'équipement micro-informatique se soit banalisé, certains groupes, plutôt jeunes et favorisés, demeurent mieux équipés que d'autres. Les écarts selon l'âge, le diplôme, les revenus et le nombre de personnes dans le logement sont très importants, comme le montrent les graphiques suivants.

Graphique 16 - Proportion de personnes disposant à domicile d'un micro-ordinateur en fonction de l'âge, du diplôme, des revenus du foyer, de la taille du foyer et du lieu de résidence



Source : CREDOC, Enquête sur les « Conditions de vie et les Aspirations des Français », juin 2010.

Quatre critères discriminants se trouvent, en 2010, à peu près au même niveau pour expliquer les inégalités d'équipement en ordinateur à domicile : l'âge, la catégorie socioprofessionnelle (CSP), le diplôme et les revenus. La taille de l'agglomération de résidence joue en revanche un rôle négligeable.

Il est intéressant de constater qu'en 2005, cinq ans plus tôt, c'était la CSP (22 %) ou le diplôme (20 %) qui, au premier chef, expliquaient les écarts d'équipement. En cinq ans, les écarts liés à la CSP ou au diplôme se sont résorbés (respectivement de 8 points et 6 points) et ils sont dorénavant moindres que les écarts liés à l'âge. Pour ce critère, la baisse n'est que de 4 points.

En revanche, l'équipement à Paris et dans son agglomération n'est que très légèrement supérieur à ce qu'il est en zone rurale (83 %, contre 72 %).

Les écarts, déjà importants s'agissant d'accès à un micro-ordinateur, sont plus criants encore lorsqu'on s'intéresse aux ordinateurs portables :

— les 18-24 ans sont les mieux pourvus (63 %), très loin devant les 70 ans et plus (11 %) ou même les sexagénaires (29 %) ;

— entre les non-diplômés (15 %) et les diplômés du supérieur (65 %), les écarts vont de 1 à 4 ;

— entre les bas revenus (33 %) et les hauts revenus (64 %), on mesure un écart allant du simple au double ;

— enfin, 56 % des habitants de Paris et son agglomération disposent, à leur domicile, d'un micro-ordinateur portable, contre 35 % dans le rural.

C. LES INÉGALITÉS D'ÉQUIPEMENT EN CONNEXION À INTERNET À DOMICILE

En 2010, près des trois quarts de la population – 71 % exactement – disposent d'une connexion à Internet à domicile. La progression constante de la diffusion d'Internet n'empêche pas un certain nombre d'inégalités de perdurer. L'âge, le niveau de diplôme, les revenus ou la taille du foyer sont là encore autant de facteurs qui influent sur l'accès à Internet à domicile. S'agissant de l'accès à Internet à domicile, l'étude 2010 du CREDOC révèle que l'implantation géographique joue un rôle très secondaire.

L'écart le plus net semble provenir de l'âge : alors que 94 % des 12-17 ans peuvent se connecter à domicile, seul un quart des 70 ans et plus a cette possibilité.

Entre les non-diplômés (35 %, moins 1 point par rapport à 2009) et les personnes issues de l'enseignement supérieur (90 %, + 4 points), l'écart s'est même creusé en 2010.

Le niveau des revenus du foyer joue aussi : moins de la moitié des personnes dont les revenus ne dépassent pas 1 500 euros par mois sont équipées, alors que plus de 90 % des personnes vivant dans un foyer dont les revenus mensuels dépassent 3 100 euros le sont.

Aujourd'hui, la quasi-totalité des connexions à Internet à domicile sont à haut débit (seuls 2 % des abonnés disposent encore d'une connexion à bas débit). L'ADSL est le mode d'accès privilégié depuis plus de cinq ans et domine largement les autres technologies d'accès : 92 % des connexions se font par l'ADSL. La fibre optique et le câble demeurent à ce jour encore peu diffusés et peinent à trouver leur clientèle.

Même si l'accès au haut débit est désormais très répandu, 44 % des personnes équipées affirment avoir, assez souvent voire très souvent, l'impression que leur connexion n'est pas assez rapide.

Selon les groupes de population, l'ancienneté de la connexion est plus ou moins grande. Les hauts revenus (73 %, + 19 points par rapport à la moyenne), les cadres (68 %), les diplômés du supérieur (66 %) ont depuis longtemps (cinq ans au moins) équipé leurs domiciles d'un accès à internet. À l'inverse, les revenus plus modestes (35 %), les non-diplômés (34 %), les personnes seules (32 %) ou encore les ouvriers (31 %) se sont équipés beaucoup plus récemment.

Pour plus de la moitié des personnes interrogées qui ne disposent pas, à domicile, d'une connexion à Internet, la raison est qu'Internet ne les intéresse pas (53 %). Plus la personne est âgée et plus le manque d'intérêt pour Internet est patent : 72 % des retraités et 74 % des plus âgés affirment que l'absence de connexion résulte d'un manque d'intérêt.

Les considérations économiques viennent ensuite : 12 % disent que l'achat d'un ordinateur est trop coûteux tandis que 9 % évoquent la cherté de l'abonnement. Au total, pour 21 % des personnes qui ne sont pas équipées, c'est l'argument du coût qui prévaut. Pour les employés (43 %), les 40-59 ans (37 %) ou les bas revenus (32 %), les contraintes budgétaires pèsent davantage encore.

Pour 10 %, enfin, c'est la complexité de l'outil qui serait un obstacle à l'équipement.

On peut relever que si depuis quelques années, la situation des étudiants vis-à-vis de l'accès à Internet s'est améliorée, il resterait néanmoins environ un étudiant sur dix qui n'a pas d'accès à Internet chez lui et qui ne peut pas, non plus, se connecter sur son lieu d'études, ce qui reste considérable.

D. LES INÉGALITÉS D'USAGE

L'étude du CRÉDOC montre que plus la personne est diplômée et plus son usage d'Internet est intense.

Les diplômés du supérieur se distinguent par des usages plutôt pratiques, les peu diplômés choisissant des pratiques plus récréatives.

On constate également un certain clivage dans le type d'usage qui est fait d'Internet en fonction des revenus du foyer : les loisirs intéressent davantage les bas revenus alors que les hauts revenus se concentrent sur des usages plus opérationnels. Enfin, on devine l'influence de l'ancienneté d'équipement sur l'intensité des usages : les personnes équipées depuis 5 ans tendent à avoir des pratiques plus denses.

Les personnes qui disposent d'une connexion déclarent passer presque autant de temps sur Internet que devant leur télévision (15 heures par semaine

pour Internet, contre 17 heures par semaine pour la télévision). Et parmi les plus diplômés, les cadres et les professions intellectuelles supérieures, ainsi que parmi les adolescents, la balance penche clairement en faveur d'Internet.

Recourir à Internet pour accomplir des démarches administratives ou fiscales est un acte de plus en plus répandu : 23 millions de personnes, soit 43 % des personnes interrogées (ou 58 % des internautes), l'ont fait au cours des douze derniers mois. Deux millions de personnes supplémentaires par rapport à l'an dernier ont donc utilisé le Web à des fins administratives.

Pour autant, tous les Français n'utilisent pas avec la même facilité Internet pour entrer en contact avec l'administration. Les écarts sont même substantiels, puisque les taux s'échelonnent entre 7 % et 86 %.

70 % des individus entre 25 et 39 ans d'âge font des démarches de ce type. Avant 18 ans et après 70 ans, en revanche, moins de 10 % des individus sont concernés.

Plus la personne est diplômée et plus elle a de chances d'effectuer tout ou partie de ses démarches administratives ou fiscales grâce à Internet : 14 % des non-diplômés le font, contre 77 % des plus diplômés.

L'écart est moindre, mais sensible tout de même, avec le niveau de revenus : on est bien moins coutumier du fait en bas de l'échelle des revenus (30 %) qu'en haut (67 %).

Enfin, à Paris et dans son agglomération, on privilégie davantage ce type de relations avec l'administration qu'en zone rurale (50 %, + 11 points par rapport aux agglomérations de moins de 2 000 habitants).

La relation avec les revenus est linéaire : plus les revenus du foyer augmentent et plus ses membres sont enclins à effectuer sur Internet les démarches administratives courantes.

Malgré la diffusion croissante d'Internet et le nombre toujours plus important d'internautes dans notre pays, beaucoup perçoivent encore des freins à l'utilisation du Web.

Depuis que le CRÉDOC interroge les Français à ce sujet, le fait que les données personnelles n'y sont pas suffisamment protégées arrive toujours en tête des raisons invoquées. En 2010, cette menace pèse davantage encore dans les esprits : 29 % des répondants citent cette raison, soit 6 points de plus que l'an dernier. La complexité d'utilisation arrive en second (12 % des réponses, - 4 points en un an), devant le problème du coût (10 %, + 1 point) et le manque d'utilité du produit (9 %, - 2 points). Arrivent ensuite les problèmes liés à la qualité de la prestation fournie : le service après-vente et l'assistance sont pointés du doigt par 7 % des personnes interrogées.

II. ATTÉNUER LA FRACTURE GÉOGRAPHIQUE

A. GÉNÉRALISER L'ACCÈS AU HAUT DÉBIT

M. Jean-Ludovic Silicani, président de l'Autorité de régulation des communications électroniques et des postes (ARCEP), lors de son audition par la mission le 30 juin 2010, a rappelé que la révolution numérique devait permettre au plus grand nombre d'accéder dans des conditions satisfaisantes au haut débit ainsi qu'au très haut débit.

S'agissant du haut débit fixe (ADSL), la France se caractérise par une des meilleures offres en Europe en termes de rapport qualité-prix et ce, pour deux raisons : des fournisseurs d'accès Internet dynamiques et une régulation efficace.

Ainsi, presque 100 % de la population française est aujourd'hui raccordable à l'Internet haut débit fixe et deux tiers des foyers français ont souscrit un abonnement ADSL. L'ARCEP entend poursuivre ses efforts afin de couvrir les dernières zones blanches de l'Internet haut débit fixe.

S'agissant du haut débit mobile (Internet 3G), le territoire français est actuellement couvert par trois réseaux (Bouygues Télécom, SFR, Orange). À la fin de l'année 2009, l'ARCEP a mis en demeure Orange et SFR de déployer leur réseau 3G, conformément aux engagements qu'ils avaient initialement pris auprès du régulateur. Un quatrième réseau devrait prochainement voir le jour, grâce à la licence qui a été récemment attribuée à Free. En 2013, 99 % de la population française sera couverte par l'Internet 3G.

B. PRÉVENIR AU MAXIMUM UNE NOUVELLE FRACTURE DANS LE DÉVELOPPEMENT DU TRÈS HAUT DÉBIT

S'agissant du très haut débit fixe, il sera l'infrastructure essentielle de la société de l'information de demain. On doit cependant constater que le déploiement d'un réseau à très haut débit sur l'ensemble du territoire exigera des investissements considérables, sans commune mesure avec l'introduction du haut débit qui a utilisé les possibilités offertes par le réseau téléphonique existant. Un rapport du cabinet IDATE a évalué le coût des investissements nécessaires à 40 milliards d'euros. Le risque est donc grand que le déploiement du très haut débit fixe n'engendre une fracture importante et durable.

On estime en effet que le jeu naturel du marché laisserait en marge du très haut débit 60 % de la population, soit plus de 80 % du territoire national, ce qui est inacceptable. D'où l'absolue nécessité de mener dans ce domaine une stratégie nationale volontariste impliquant l'État, les acteurs privés et les collectivités territoriales.

L'ARCEP, en application de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie et de la loi n° 2009-1572 du 17 décembre 2009

relative à la lutte contre la fracture numérique, est chargée de préciser les conditions de déploiement de la fibre optique.

En décembre 2009, l'Autorité a pris une décision en ce sens pour les zones très denses. Sur cette base, les opérateurs ont rendu publiques leurs offres d'accès en février 2010 et ont annoncé les premiers programmes d'investissement en fibre optique en avril 2010, qui couvrent potentiellement 800 000 foyers.

M. Jean-Ludovic Silicani avait indiqué à la mission que l'ARCEP travaillait, par ailleurs, à l'élaboration du cadre réglementaire de la fibre optique pour les zones moins denses.

En décembre 2010, l'Autorité a ainsi pris deux décisions pour le déploiement des réseaux à très haut débit dans les régions françaises faiblement peuplées, dans lesquelles le déploiement de la fibre optique ne pourra se faire sans l'intervention des collectivités territoriales.

La première définit un cadre qui entend favoriser les partenariats public-privé. L'objectif est de faciliter le co-investissement en permettant aux acteurs publics et privés d'étendre leurs investissements à l'ensemble du territoire et de favoriser la « mutualisation ». Les zones moins denses se caractérisant par une appétence bien plus faible des acteurs privés à investir, il s'agit d'encourager ces derniers à fournir leurs services très haut débit en s'appuyant sur une même boucle locale en fibre optique.

La seconde décision établit les règles d'éligibilité aux aides du fonds d'aménagement numérique des territoires créé en 2009 par la loi relative à la lutte contre la fracture numérique et alimenté par les deux milliards d'euros du grand emprunt destinés à l'accélération du déploiement du très haut débit en zones rurales.

L'objectif est double :

— créer un véritable effet de levier sur l'investissement privé tout en favorisant le co-investissement des différents acteurs, via la mise à disposition des opérateurs de ressources financières non bonifiées mais de longue maturité adaptées à la durée de vie de ces nouveaux réseaux en fibre optique ;

— et soutenir simultanément, par un cofinancement de l'État, les projets d'aménagement numérique portés par les collectivités territoriales et s'inscrivant en complémentarité avec ceux des opérateurs, dans des conditions prévues par la loi de 2009 relative à la lutte contre la fracture numérique.

Ces deux décisions doivent permettre de tendre vers l'objectif fixé par l'Union européenne, qui consiste à atteindre une couverture totale en très haut débit d'ici 2020.

La France est aujourd'hui le premier pays en Europe à disposer d'un cadre réglementaire complet et cohérent définissant les conditions que devront respecter les opérateurs privés et les collectivités publiques pour le déploiement des réseaux de fibre optique sur l'ensemble du territoire. Le principe est que moins les zones seront denses et rentables, plus le degré de mutualisation des réseaux et des moyens sera important. À cet égard, les acteurs privés comme publics sont informés et désireux d'agir, à l'instar des collectivités locales qui font montre d'un dynamisme certain en la matière. L'ARCEP souhaite, pour sa part, que les opérateurs investissent dans les réseaux afin de permettre le bon fonctionnement de cette économie numérique.

Il importe aussi que les collectivités territoriales soient soutenues dans leur démarche active en vue du déploiement de la fibre optique. À cet égard, on pourrait imaginer des mécanismes de péréquation permettant d'agir en faveur des collectivités les plus menacées par la fracture numérique territoriale.

S'agissant du très haut débit mobile (Internet 4G), M. Silicani avait annoncé à la mission que l'ARCEP en attribuerait les fréquences au premier semestre de l'année 2011. Conformément à ce calendrier, l'Autorité a rendu public, le 16 mai 2011, les projets de décisions concernant les procédures d'attribution des fréquences 4G. Les conditions d'attribution de ces fréquences visent notamment à satisfaire l'objectif de lutte contre la fracture numérique, conformément aux dispositions de la loi précitée relative à la lutte contre la fracture numérique qui prévoit que le dividende numérique prend en compte de manière prioritaire l'aménagement du territoire. Des objectifs de couverture sont fixés au plan national : 99,6 % de la population métropolitaine devra ainsi être couverte par chaque opérateur. Et pour la première fois, des objectifs de couverture sont également inscrits au plan départemental. En outre, une zone de déploiement prioritaire, correspondant aux territoires peu denses (18 % de la population et 63 % de la surface du territoire), fait l'objet d'un calendrier de déploiement accéléré. Ce déploiement devrait être facilité par des mesures incitant à la mutualisation des réseaux et des fréquences, entre opérateurs. Il s'agit d'une mesure importante car le très haut débit mobile pourra être accessible plus rapidement que le très haut débit fixe dans les territoires peu denses.

C. COMBINER LES DIFFÉRENTES TECHNOLOGIES DISPONIBLES POUR AMÉLIORER LE DÉBIT DISPONIBLE SUR L'ENSEMBLE DU TERRITOIRE

La fibre n'est pas la seule technologie utilisable pour aller au-delà du « haut débit » actuellement disponible.

En application de la loi précitée de lutte contre la fracture numérique, les régions et les départements vont élaborer des schémas directeurs de l'aménagement numérique du territoire.

L'ARCEP a remis au Parlement, en septembre 2010, un rapport sur l'ensemble des technologies existantes et leur possible articulation en vue de

déployer le haut et le très haut débit sur l'ensemble du territoire par des réseaux fixes, mobiles ou satellitaires.

En attendant le déploiement d'un réseau de très haut débit, fixe et/ou mobile, sur des parties significatives du territoire, la montée en débit du réseau haut débit existant constitue une solution techniquement envisageable et économiquement viable d'offrir une réponse à des consommateurs désireux de débits plus importants à court terme.

Les opérateurs de communication électronique ont annoncé ou lancé le déploiement de nouveaux réseaux d'accès permettant d'accroître considérablement les débits et s'appuyant sur la mise en place de nouvelles boucles locales en fibre optique (réseaux FTTH), la rénovation des réseaux câblés et le développement du futur réseau de très haut débit mobile (LTE) [(1)].

Les réseaux de desserte sans fil offrent des alternatives qui, sur certaines zones, pourraient être plus rentables que la fibre, sans toutefois présenter les mêmes qualités techniques :

— le Wi-Fi présente des coûts réduits de développement. À ce titre il pourrait être utilisé pour desservir certaines zones rurales. Il permet la transmission de données par ondes radio avec des débits pouvant aller jusqu'à 25 Mb/s, sur des zones de plusieurs dizaines de mètres ;

— le WiMax couvre des surfaces de l'ordre de plusieurs kilomètres : un émetteur relié à une liaison très haut débit diffuse un signal de plusieurs dizaines de Mb/s, partagé entre les utilisateurs finaux ;

— enfin, une desserte par satellite présente l'avantage de desservir tous les territoires non couverts par les autres technologies. S'il existe aujourd'hui des offres à haut débit par satellite, cette solution présente plusieurs inconvénients majeurs : le débit doit être partagé entre tous les utilisateurs, les coûts d'équipements (modem et antenne parabolique) sont importants et les transmissions présentent un temps de latence élevée qui rend plus difficiles certains usages.

La technologie la plus porteuse d'espérances pour les zones rurales est peut-être toutefois, au cours des années à venir, le LTE (*Long Term Evolution)*, technologie de réseaux mobiles de quatrième génération. Cette technologie offrira des débits supérieurs au haut débit fixe actuel, et sera accessible dans les zones rurales. Si cette technologie n'offre pas les mêmes qualités que la fibre optique, elle peut permettre aux territoires ruraux d'accéder, à un coût réaliste et à un horizon raisonnable, aux services Internet de demain.

*(1) Le LTE (*Long Term Evolution*) est la technologie de réseau mobile qui devrait succéder à la 3G. Le LTE apportera un certain nombre d'améliorations par rapport aux réseaux 3G classiques, à commencer par des débits nettement supérieurs. Le LTE est notamment attendu pour désengorger le réseau 3G.*

Orientation n° 44 : réduire la fracture numérique territoriale

— La mission souhaite que des mécanismes de soutien soient mis en œuvre par exemple sous forme de dispositifs de péréquation en faveur des territoires menacés par la fracture numérique territoriale ;

— la mission souhaite aussi que soit exploré l'ensemble des opportunités offertes par toutes les technologies disponibles afin d'améliorer la desserte des territoires, en attendant le déploiement effectif de la fibre.

III. LA LUTTE CONTRE LA FRACTURE SOCIALE ET CULTURELLE

A. METTRE EN PLACE UNE TARIFICATION SOCIALE DE L'INTERNET

La mission souhaite la mise en place d'une véritable tarification sociale de l'Internet. Cette dernière suppose néanmoins une modification de la directive correspondante afin que l'accès à Internet à haut débit devienne une composante du service universel des communications électroniques, comme le souligne le rapport du Centre d'analyse stratégique, *Le fossé numérique en France,* remis le 20 avril 2011 au Parlement, en application de l'article 25 de la loi n° 2009-1572 du 17 décembre 2009 relative à la lutte contre la fracture numérique.

Le 18 janvier 2010, le Premier ministre, M. François Fillon, a encouragé les opérateurs télécoms à proposer une « offre sociale » aux plus démunis, leur permettant d'accéder à l'Internet à haut débit pour un prix mensuel d'environ 20 euros. « *Je souhaite que d'ici six mois, tous les opérateurs qui le souhaitent puissent proposer une offre sociale spécifique pour permettre aux foyers les plus modestes d'accéder à Internet dans des conditions attractives. Cette offre sociale devrait être aux alentours de 20 euros*, » a-t-il détaillé. « *À cette fin, j'ai demandé au ministre de l'Industrie de mener les consultations nécessaires pour engager une modification du code des postes et communications électroniques, afin de permettre d'offrir à tous les opérateurs la faculté de mettre en place une telle offre*. »

En France, la plupart des opérateurs, répondant aux vœux ainsi exprimés, proposent désormais des offres Internet haut débit pour moins de 20 euros mais ces tarifs ne sont accessibles que dans les grandes villes. Or, on ne peut pas concevoir un tarif social à plusieurs vitesses selon que l'on habite à la ville ou à la campagne.

Dès lors, il convient, en modifiant la loi, d'élargir la notion de service universel [(1)] des communications électroniques à l'Internet haut débit. Il s'agit de garantir un accès de tous au réseau à un prix raisonnable en permettant à l'État

(1) Le service universel garantit à tous l'accès *« au réseau de communications public (...) à un prix abordable. Cette exigence s'applique à la fourniture (...) de communication de données à des débits suffisants pour accéder à des services en ligne tels que ceux qui sont proposés sur le réseau Internet public* » (directive 2009/136/CE du 25 novembre 2009).

d'imposer aux opérateurs la mise en place d'un tarif social de l'Internet « *prenant en compte les difficultés particulières rencontrées (...) par certaines catégories de personnes, en raison notamment de leur niveau de revenu* » [(1)].

Cette extension n'est toutefois pas envisageable sans une modification de la directive 2009/136/CE du 25 novembre 2009 qui définit le service universel des communications électroniques mais n'intègre pas aujourd'hui les services Internet à haut débit dans son champ. Ce texte est en cours de révision : la Commission européenne a lancé le 2 mars 2010 une consultation publique visant à déterminer les conditions d'un tel élargissement à l'ensemble de l'Union européenne. Elle devrait en présenter les conclusions dans le courant du premier trimestre 2011 et indiquer les modifications de la directive qu'elle envisage.

Rappelons que le service universel des communications électroniques, dans son périmètre actuel, garantit à tous, en France, l'accès aux services de communication de base, considérés comme essentiels pour la participation des citoyens à la vie économique et sociale. L'Internet à haut débit ne figure pas dans le périmètre des services universels pris en charge par le fonds de service universel alimenté par les opérateurs. La directive 2009/136/CE du 25 novembre 2009 précise que cette situation ne permet pas l'instauration d'un tarif social sur les services Internet à haut débit.

Peut être chargé de fournir l'une des composantes du service universel « *tout opérateur en acceptant la fourniture sur l'ensemble du territoire national et capable de l'assurer* » aux termes de l'article L. 35-2 du CPCE. La désignation du ou des opérateurs en charge du service universel est faite par le ministre en charge des communications électroniques, par appel à candidatures portant sur les conditions techniques et tarifaires ainsi que, le cas échéant, le coût net de fourniture de ces prestations. Les coûts nets imputables aux obligations de services universels, évalués sur la base d'une comptabilité appropriée tenue par les opérateurs désignés pour assurer ces obligations, sont financés par un fonds de service universel des communications électroniques alimenté par les opérateurs au prorata de leur chiffre d'affaires réalisé au titre des services de communications électroniques.

Orientation n° 45 : permettre un accès au haut débit à bas coût pour les plus démunis

La mission souhaite la mise en place d'une véritable tarification sociale de l'Internet, ce qui suppose néanmoins une modification de la directive 2009/136/CE du 25 novembre 2009 afin que l'accès à Internet à haut débit devienne une composante du service universel des communications électroniques.

(1) Article L. 35-1 du code des postes et des communications électroniques.

B. DÉVELOPPER LE RÉSEAU D'ESPACES PUBLICS NUMÉRIQUES

La mission souhaite que soit poursuivi le déploiement du réseau d'espaces numériques publics (EPN).

Les espaces publics numériques (EPN) assurent un service gratuit d'accès à Internet et d'accompagnement du grand public à l'utilisation des outils et usages numériques. Ils sont implantés dans des structures culturelles ou sociales telles que bibliothèques, médiathèques, centres socioculturels ou maisons des jeunes. La France compte aujourd'hui plus de 4 000 espaces qui contribuent à la démocratisation de l'accès public à Internet.

Il existe trois grands réseaux nationaux d'EPN :

— le réseau des Espaces culturels multimédias (ECM), soutenus par le ministère de la Culture ;

— le réseau des Points Cyb, du ministère de la Jeunesse et des sports ;

— le réseau Cyber-base, lancé par la Caisse des dépôts et consignations. Ce dernier couvre près des trois quarts des départements, représente plus de 830 sites, reçoit 2 millions de visites par an, et dispose de 1 800 animateurs.

Ces dispositifs nationaux s'interpénètrent souvent au niveau local avec les initiatives des collectivités territoriales. Depuis 1998, la majorité des régions et de nombreuses collectivités ont en effet mis en place des espaces publics multimédias qui maillent le territoire. Ces espaces comportent un ou plusieurs animateurs qui accompagnent, initient, aident chacun à maîtriser et bien utiliser ces outils et les services offerts par Internet.

L'étude 2010 du CRÉDOC fait d'ailleurs apparaître une forte demande d'accompagnement pour mieux utiliser les outils informatiques.

34 % de nos concitoyens déclarent ainsi qu'ils seraient prêts à se rendre dans des lieux publics proches de chez eux où ils pourraient trouver des personnes pouvant les aider à utiliser un ordinateur ou Internet. Il faut en effet savoir que 47 % de la population ne se sentent pas compétents pour utiliser un ordinateur (même parmi les équipés, une personne sur trois avoue des difficultés). Le besoin d'accompagnement touche tous les groupes : 34 % de ceux qui ne sont pas encore équipés en Internet en font état, tout comme 40 % de ceux qui sont équipés depuis peu et même 30 % de ceux qui disposent chez eux d'Internet depuis plus de 5 ans.

Orientation n° 46 : poursuivre le déploiement du réseau d'espaces numériques publics (EPN) et développer, en leur sein, l'accompagnement du public dans l'usage des technologies numériques

La mission estime qu'il s'agit d'un moyen efficace de réduire l'inégalité numérique dont sont victimes les personnes ne disposant pas d'ordinateur, d'accès au réseau ou de la connaissance technique nécessaire pour les utiliser.

C. DÉVELOPPER LE B2I ADULTES

Dans sa contribution écrite aux réflexions de la mission, la Ligue de l'enseignement rappelle que « *pour contribuer à la formation citoyenne de l'ensemble de la population en matière de compréhension et d'usages des outils numériques, la Ligue de l'enseignement et d'autres associations interviennent dans différents lieux publics : Maisons de quartiers, Espaces publics numériques (EPN), maisons de retraite… Elles devraient pouvoir contribuer à la formation au B2i adultes, récemment réorganisée, mais il est nécessaire pour cela de préciser les textes officiels.* »

Le B2i adultes s'adresse à tous les publics adultes en formation (générale, professionnelle ou spécifique à l'usage des TIC) ou en situation professionnelle. Il est utile aux salariés et aux demandeurs d'emploi pour se former et progresser, pour indiquer dans un CV leur niveau de maîtrise, pour avoir la garantie d'une attestation de compétences reconnue par l'Éducation nationale. Depuis mai 2010, le B2i adultes a été profondément rénové pour s'adapter à la recommandation du Parlement et du Conseil de l'Union européenne sur les compétences clés. Pour obtenir le B2i adultes, les candidats doivent apporter la preuve de leurs compétences en fournissant « un dossier de preuves ». Seuls les organismes agréés peuvent délivrer le B2i adultes. Les recteurs d'académie sont chargés d'examiner les demandes d'agrément déposées par les organismes de formation.

Orientation n° 47 : développer le B2i adultes

Comme la Ligue de l'enseignement, la mission estime qu'« *en attendant que toute la population soit passée par les formations B2i École, Collège et Lycée, le B2i adultes est en effet une réponse au problème de la fracture numérique qui touche toutes les générations.* »

D. MULTIPLIER LES INITIATIVES PERMETTANT DE METTRE DES ORDINATEURS À DISPOSITION DES PERSONNES QUI N'EN DISPOSENT PAS

Parmi les initiatives intéressantes, on peut relever la mise en place dans les logements sociaux d'ordinateurs connectés. Il s'agit d'une initiative encore limitée mais qui se développe à l'instigation des collectivités locales et des bailleurs sociaux. Des ensembles de logements sociaux ont été dotés d'ordinateurs et d'accès Internet haut débit dont le coût, plus faible qu'un abonnement normal, est compris dans les charges. De tels projets ont vu le jour à Angers, Angoulême, Brest, etc. La plupart sont encore en phase d'expérimentation. Le secrétaire d'État chargé du Logement se propose d'élargir cette initiative et de mettre en place un label « Logement social numérique ». Il vise à encourager les bailleurs à équiper les logements sociaux en accès aux technologies numériques et permettre ainsi le développement de l'Internet haut débit dans le parc HLM français. Les financements de l'État accordés à ces projets devraient dépendre de la qualité de cet environnement numérique.

Des initiatives telles que la mise à disposition des familles défavorisées d'ordinateurs, comme c'est le cas en France *via* l'expérience « ordi 2.0 », constituent également une piste intéressante à développer. Lancée en juin 2008, l'opération « ordi 2.0 » consiste à reconditionner des ordinateurs pour les ménages à revenus modestes. Ce programme a aidé en 2010 plus de 35 000 foyers à s'équiper en ordinateurs. La réutilisation des ordinateurs constitue une réponse d'urgence, facile à mettre en œuvre, à des conditions avantageuses pour les personnes en difficulté sociale, économique ou culturelle. De nombreuses initiatives des pouvoirs publics et d'associations avaient déjà été prises en ce sens : certaines collectivités locales se sont engagées depuis longtemps, dans la redistribution des ordinateurs de seconde main aux collégiens, ou dans l'installation d'ordinateurs rénovés dans l'habitat social.

Enfin, il convient de rappeler que le don d'ordinateurs d'occasion et de logiciels au salarié par l'employeur a été exonéré d'impôt sur le revenu et de cotisations de sécurité sociale dans la limite de 2 000 euros par an par l'article 31 de la loi de finances pour 2008. Ce régime fiscal et social de faveur a pour objectif d'encourager le don de matériels informatiques par les employeurs à leurs salariés.

Orientation n° 48 : favoriser et développer les initiatives permettant de mettre des ordinateurs à disposition des personnes qui n'en disposent pas à travers :

– la mise en place dans les logements sociaux d'ordinateurs connectés ;

– la mise à disposition des familles défavorisées des ordinateurs reconditionnés.

E. MIEUX PROTÉGER LES PERSONNES EN DIFFICULTÉ FINANCIÈRE RISQUANT DE PERDRE LEUR CONNEXION À INTERNET

1. Ne pas permettre la saisie des ordinateurs personnels dans le cadre d'une procédure d'exécution

Les personnes qui se trouvent dans une situation de surendettement telle que leurs biens mobiliers font l'objet d'une saisie peuvent se voir privées de leur ordinateur si celui-ci n'est pas utilisé comme un instrument de travail nécessaire à l'exercice personnel de l'activité professionnelle.

Cette interprétation de l'article 14 de la loi n° 91-650 du 9 juillet 1991 portant réforme des procédures civiles d'exécution a été confirmée par les services du ministère de la Justice à l'occasion d'une réponse à une question écrite [(1)] du président de notre mission, M. Jean-Luc Warsmann, qui, dès 2003, s'inquiétait de la possibilité que soient saisis des ordinateurs contenant des données personnelles. Le ministère de la Justice avait alors répondu que les délais de la procédure *« rendent impossible l'enlèvement par surprise de l'ordinateur dans des*

(1) Question n° 21239.

conditions qui priveraient le débiteur de la possibilité d'imprimer ou de sauvegarder les informations stockées sur son disque dur. »

On peut cependant s'interroger sur le sens qu'il y a à recourir à des sauvegardes informatiques si la personne n'a plus l'ordinateur pour en lire le contenu ; mais, surtout, il convient de constater qu'un ordinateur est devenu avant tout un outil de connexion au réseau, nécessaire pour exercer ses droits, accéder à la culture et rester en lien avec le monde du travail.

Les dispositions légales relatives aux biens insaisissables relèvent d'une époque antérieure à la révolution numérique. Un ordinateur peut ne pas être, au sens strict *« un instrument de travail nécessaire à l'exercice personnel de l'activité personnelle* » ou être utilisé *« pour la poursuite des études ou la formation professionnelle* », selon les catégories définies par le décret du 31 juillet 1992 [(1)], tout en demeurant indispensable, pour chercher un emploi, obtenir rapidement des renseignements administratifs ou exercer son droit d'expression.

La liste des besoins fondamentaux ne saurait être considérée comme figée. Elle est amenée à évoluer. Le décret du 31 juillet 1992 a d'ailleurs déjà été complété, en 1997 [(2)], par l'ajout à la liste des biens insaisissables d'un poste téléphonique permettant l'accès au service téléphonique fixe.

Pour ces raisons, la mission d'information considère qu'il serait utile de compléter la liste des « *biens nécessaires à la vie et au travail du saisi et de sa famille* » en y ajoutant la mention d'un ordinateur individuel.

Par analogie avec la disposition portant sur le maintien d'un poste téléphonique, cette mesure exclurait de la procédure de saisie un poste d'ordinateur pour l'ensemble du foyer concerné.

Orientation n° 49 : garantir à l'internaute qu'il ne sera pas dépossédé de son ordinateur personnel dans le cadre d'une procédure de saisie

Ajouter à la liste des biens insaisissables, telle que l'a fixée le décret du 31 juillet 1992, la mention de l'ordinateur personnel afin que les personnes faisant l'objet d'une saisie mobilière ne se voient pas fermer l'accès au monde numérique.

(1) Article 39 du décret n° 92-755 du 31 juillet 1992 : « Pour l'application de l'article 14 (4°) de la loi du 9 juillet 1991, sont insaisissables comme étant nécessaires à la vie et au travail du débiteur saisi et de sa famille : les vêtements ; la literie ; le linge de maison ; les objets et produits nécessaires aux soins corporels et à l'entretien des lieux ; les denrées alimentaires ; les objets de ménage nécessaires à la conservation, à la préparation et à la consommation des aliments ; les appareils nécessaires au chauffage ; la table et les chaises permettant de prendre les repas en commun ; un meuble pour abriter le linge et les vêtements et un meuble pour ranger les objets ménagers ; une machine à laver le linge ; les livres et autres objets nécessaires à la poursuite des études ou à la formation professionnelle ; les objets d'enfants ; les souvenirs à caractère personnel ou familial ; les animaux d'appartement ou de garde ; les animaux destinés à la subsistance du saisi, ainsi que les denrées nécessaires à leur élevage ; les instruments de travail nécessaires à l'exercice personnel de l'activité professionnelle ; un poste téléphonique permettant l'accès au service téléphonique fixe. »

(2) Décret n° 97-375 du 17 avril 1997.

2. Assouplir les clauses contractuelles relatives à l'arrêt des connexions à Internet en cas de retard de paiement

D'autres initiatives que celles mentionnées précédemment concernant la mise en place d'une tarification sociale de l'Internet pourraient être mises à l'étude. Les conditions dans lesquelles les services de connexion à Internet sont interrompus pour défaut de paiement, pourraient, par exemple, être réévaluées. Les principaux fournisseurs d'accès laissent actuellement à l'abonné un délai qui varie de 8 à 15 jours après mise en demeure. Si l'on considère l'accès à Internet comme un service présentant le même degré de nécessité que la fourniture d'eau, de gaz et d'électricité ou que la connexion au réseau téléphonique, des délais plus larges sembleraient envisageables.

La procédure suivie lorsqu'un consommateur d'électricité, de gaz, de chaleur ou d'eau n'a pas acquitté sa facture est la suivante : aux termes de l'article premier du décret n° 2008-780 du 13 août 2008, dans un délai de 14 jours après la date d'émission de la facture ou à la date limite de paiement, lorsque cette date est postérieure, le fournisseur informe le consommateur par un premier courrier qu'à défaut de règlement dans un délai supplémentaire de 15 jours sa fourniture pourra être réduite ou suspendue pour l'électricité ou suspendue pour le gaz, la chaleur ou l'eau. Le décret précise qu'à défaut d'accord entre le consommateur et le fournisseur sur les modalités de paiement dans le délai supplémentaire de 15 jours, ce dernier peut procéder à la réduction ou à la coupure et en avise le consommateur au moins 20 jours à l'avance par un second courrier.

Il est à noter que ce dispositif prend en compte le cas des personnes en situation précaire. L'article L. 115-3 du code de l'action sociale et des familles leur ouvre en effet, un droit à une aide de la collectivité pour disposer de la fourniture d'eau, d'énergie et de services téléphoniques dans leur logement. Cet article dispose, en outre, qu'en cas de non-paiement des factures, *« la fourniture d'énergie, d'eau ainsi que d'un service téléphonique restreint est maintenue jusqu'à ce qu'il ait été statué sur la demande d'aide. Le service téléphonique restreint comporte la possibilité, depuis un poste fixe, de recevoir des appels ainsi que de passer des communications locales et vers les numéros gratuits, et d'urgence.* » La fourniture d'énergie ne peut être interrompue du 1er novembre de chaque année au 15 mars de l'année suivante.

De manière analogue, le maintien d'un accès au réseau pourrait être proposé aux personnes qui, exceptionnellement, se trouvent dans une situation ne leur permettant pas de régler leur facture d'abonnement. Cette aide, fournie par la collectivité, s'inscrirait parmi les dispositions relatives à la lutte contre la pauvreté et les exclusions figurant dans le code de l'action sociale et des familles. Un tel dispositif serait lié à des conditions de revenus. Le débit assuré devrait être suffisant pour accéder dans des conditions normales aux différents services en ligne (1).

(1) Selon l'OCDE, le seuil minimal de haut débit est de 256 kbits/s.

L'impact financier qu'aurait l'introduction de ces mesures dans le domaine de l'accès au numérique demanderait à être évalué. En tout état de cause, la liberté d'accéder à Internet, dont le Conseil constitutionnel a reconnu la portée au regard des droits fondamentaux, s'en trouverait mieux garantie pour les personnes en difficultés.

Orientation n° 50 : aider les personnes en difficultés pour raisons financières à conserver leur accès à Internet

F. PORTER UNE ATTENTION PARTICULIÈRE AUX JEUNES QUI SONT VICTIMES DE LA FRACTURE NUMÉRIQUE

Si le fossé générationnel doit progressivement s'estomper, la situation est plus critique pour les 34 % des 15-24 ans les moins diplômés, qui n'ont souvent pas accès à Internet à leur domicile (16 %) ou qui ne maîtrisent pas cet outil.

Cette population qui éprouve souvent des difficultés de lecture risque de se trouver marginalisée dans la société numérique de demain.

Pour éviter que les enfants de parents victimes de la fracture numérique n'en soient pas victimes à leur tour, l'école a un rôle déterminant à jouer.

Le renforcement à l'école de l'aide personnalisée, et plus généralement de la lutte contre l'échec scolaire, ainsi que l'amélioration de l'accès à Internet des populations les plus défavorisées (par la mise à disposition d'ordinateurs, de tarifs d'abonnement adaptés, etc.) constituent des pistes de solution. Des formations spécifiques pourraient également être proposées à l'occasion des Journées défense et citoyenneté (JDC).

Dans tous les cas, l'existence d'une population éprouvant des difficultés de lecture et d'utilisation d'Internet implique de veiller à ce que les portails publics et les procédures administratives en ligne soient d'un accès aisé.

IV. ÉVITER LE RISQUE D'UNE MARGINALISATION ACCRUE POUR LES PERSONNES HANDICAPÉES

Le problème de l'accessibilité d'Internet pour les personnes handicapées se pose ainsi non en termes de bien-être ou de commodités mais constitue un enjeu au regard des droits fondamentaux. Les engagements précédemment cités pris à l'occasion du Sommet mondial de l'information, le 18 novembre 2005, préconisent, par exemple, un accès abordable aux technologies de l'information et de la communication, y compris aux technologies de « *facilitation* » [(1)] pour les personnes handicapées. La Convention des Nations unies du 13 novembre 2006 relative aux droits des personnes handicapées a reconnu, en son article 9, que l'accessibilité « *aux services d'information, de communication et autres services,*

(1) Cf. §18 de ce document.

y compris les services électroniques » faisait partie des mesures qui « *permettent aux personnes handicapées de vivre de façon indépendante et de participer pleinement à tous les aspects de la vie* ». L'article 21 de ce même texte invite les États à prendre toutes mesures appropriées pour que les personnes handicapées puissent exercer leur droit d'expression et d'opinion, en particulier pour les communications faites par le biais d'Internet.

La transposition du troisième « paquet télécoms » devrait aussi conduire à renforcer les dispositions en faveur des utilisateurs handicapés des services de communication électronique. La directive 2009/136/CE incite, en particulier, les États membres « *à promouvoir la création d'un marché des produits et des services de grande diffusion qui intègrent des fonctionnalités pour les utilisateurs finals handicapés* » ; elle leur demande aussi de garantir « *l'équivalence entre le niveau d'accès des utilisateurs finals handicapés aux services et le niveau offert aux autres utilisateurs finals*. [(1)] »

En l'absence d'une étude transversale portant sur les difficultés rencontrées par les personnes handicapées pour accéder à Internet, quel que soit le handicap, la mission d'information a procédé à l'audition de plusieurs associations représentant les handicapés visuels [(2)]. La France compte, en effet, 1,7 million d'handicapés visuels dont environ 100 000 aveugles. En raison du vieillissement de la population, le handicap visuel touche un nombre croissant de personnes. L'accès à Internet se faisant principalement par le biais d'écrans visuels, un risque grave de marginalisation serait encouru si des outils n'étaient pas conçus pour les aider et si des mesures d'incitation n'étaient pas prises pour améliorer l'accessibilité des sites Internet.

A. DES MOYENS EXISTENT POUR PALLIER LES DIFFICULTÉS DES INTERNAUTES HANDICAPÉS VISUELS

Les outils utilisés diffèrent selon le degré de handicap. Les personnes aveugles ont besoin d'outils spécialisés souvent coûteux. La synthèse vocale est le moyen technique le plus courant car il ne nécessite pas de formation spécifique et s'avère plutôt bon marché. La plage braille couplée à un logiciel de lecture d'écran est un outil très efficace mais cher, une plage braille de 40 caractères coûtant environ 6 000 euros, et un logiciel de lecture d'écran 1 600 euros.

Les personnes malvoyantes utilisent des logiciels qui permettent de travailler les contrastes et l'agrandissement des images ; les logiciels nécessaires représentent un coût d'environ 600 euros [(3)].

---

(1) Considérants 9 et 12 de la directive 2009/136/CE.

(2) Audition du 16 février 2011.

(3) Les personnes atteintes d'un handicap moteur peuvent utiliser des baguettes à bouche ou à tête. Des outils plus onéreux et spécialisés existent comme les dispositifs de contrôle par la respiration ou les dispositifs de suivi des yeux.

Des difficultés de lecture demeurent cependant insurmontables. Par exemple, la connexion à certains sites de banques en ligne passe par la saisie de codes sur des claviers virtuels qui sont affichés sur les écrans et, de ce fait, inutilisables par les déficients visuels ; ceux-ci sont également dans l'incapacité de recopier les cryptogrammes anti-spam que l'internaute est assez souvent obligé d'identifier pour accéder à un contenu Web.

Le principal enjeu technique, pour les handicapés visuels, est l'interopérabilité des produits informatiques mis sur le marché. Il convient en effet que les logiciels demeurent compatibles avec les dispositifs techniques qu'eux-mêmes utilisent. Les représentants des associations déplorent que trop de produits nouveaux demeurent inaccessibles parce qu'il n'a pas été tenu compte, au niveau de leur conception, de l'extension de leur système de fonctionnement aux appareils utilisés par les handicapés. Certains produits font cependant exception et peuvent servir d'exemple ; il en va ainsi des produits Apple qui intègrent les fonctionnalités techniques permettant la lecture d'écrans par les malvoyants [(1)].

L'équipement technique des personnes handicapées peut être financé par la prestation compensation du handicap (PCH), d'un montant de 3 960 euros, renouvelable tous les trois ans, et par les fonds octroyés par les maisons départementales pour personnes handicapées. Les enfants et jeunes adultes handicapés reçoivent une formation au sein des services d'aide à l'acquisition de l'autonomie et à l'intégration. La Fédération des aveugles de France déplore cependant que seuls 50 % des départements disposent de ces services d'accompagnement.

M. Fernando Pinto Da Silva, responsable du Centre d'évaluation et de recherche sur les technologies pour aveugles et malvoyants (CERTAM), a regretté que les niveaux de formation des équipes destinées à l'accompagnement des personnes déficients visuels dans les maisons départementales pour personnes handicapées soient très inégaux d'un département à l'autre et a appelé de ses vœux la mise en place d'une formation qui serait proposée au niveau national.

Concernant le monde du travail, l'association de gestion du fonds pour l'insertion professionnelle des personnes handicapées (AGEFIPH) accompagne les personnes handicapées en proposant une formation et un financement de l'adaptation des postes de travail. Une telle aide est indispensable dans un monde professionnel où l'informatique est omniprésente, notamment pour éviter le reclassement sur des postes subalternes des personnes devenues malvoyantes du fait, par exemple, d'une maladie dégénérative.

(1) Apple propose un logiciel de lecture d'écran intégré au Macbook Air, et des Iphone 3GS et 4G adaptés aux handicapés visuels.

B. LES OBLIGATIONS LÉGALES ET LEURS LIMITES

La France dispose, depuis 2005, d'une législation relative à l'accessibilité des sites Internet publics, mais aucune contrainte ne pèse sur les sites privés.

1. Les sites Internet publics

L'article 47 de la loi n° 2005-102 du 11 février 2005 visant à garantir l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées dispose que « *les services de communication publique en ligne des services de l'État, des collectivités territoriales et des établissements publics qui en dépendent doivent être accessibles aux personnes handicapées* ». Le décret d'application n° 2009-546 du 14 mai 2009 fixe un délai de mise en conformité de deux ans pour les sites d'État et de trois ans pour les sites des collectivités. Un référentiel général d'accessibilité pour les administrations (RGAA) a été approuvé par arrêté en date du 21 octobre 2009 qui précise les exigences techniques à respecter pour l'accessibilité des contenus Web.

M. Dominique Burger, président de l'association BrailleNet, a regretté que le décret d'application de l'article précité n'ait été promulgué que quatre ans après l'entrée en vigueur de la loi et qu'il s'avère si peu contraignant. Il manquerait, en particulier d'un « pilote » qui serait chargé de coordonner le projet d'accessibilité des sites publics et remplirait une fonction d'interlocuteur entre les acteurs publics, les entreprises et les usagers. Le RGAA n'a, en outre, pas été mis à jour depuis 2009 alors que le contexte technique est très évolutif. La sanction, pour les services qui ne seront pas en conformité à l'issue du délai prévu, semble également insuffisante, leur inscription sur une « liste noire » étant peu dissuasive.

Les associations appellent donc de leurs vœux la réécriture du décret du 14 mai 2009.

Par ailleurs, aux termes de l'article 6 de ce même décret, les personnels intervenant dans les services de communication publique en ligne de l'État et des collectivités territoriales doivent recevoir une formation théorique et pratique sur l'accessibilité de ces services aux personnes handicapées, afin de les rendre conformes aux règles et standards nationaux et internationaux. Or aucun bilan n'a été dressé à ce jour permettant d'évaluer la réalité de cet enseignement et son efficacité.

Un bilan d'ensemble de l'application des dispositions légales relatives à l'accessibilité, pour les personnes handicapées, des services de communication en ligne de l'État semble s'imposer.

2. Les sites Internet privés

La législation française ne prévoit aucune obligation d'accessibilité des sites Internet privés. Une procédure de labellisation est cependant possible. Les

normes fixées par le W3C [1] sont considérées par le Parlement européen comme un standard de référence [2]. Ce consortium propose une labellisation en trois niveaux, *A, AA* et *AAA,* chaque niveau attestant d'une certaine qualité d'accessibilité numérique. L'association française BrailleNet propose un processus de labellisation semblable avec trois niveaux, bronze, argent et or, appelé label AccessiWeb, et s'est associée à deux associations belges et espagnoles pour créer le label européen Euracert. M. Dominique Burger a cependant constaté qu'aucun des acteurs les plus importants d'Internet ni aucun réseau social n'avaient fait part de son intérêt pour cette labellisation.

Aux États-Unis, l'action des associations de handicapés a conduit à imposer des contraintes sur le secteur privé plus fortes qu'en Europe. Ainsi, la Fédération nationale des aveugles (NFB) a intenté en 2006 un procès, selon la procédure de « *class action* », contre le site de e-commerce *Target* pour défaut d'accessibilité de ses services en ligne. Le 27 août 2008, cette société a versé un dédommagement de six millions de dollars à la NFB et s'est engagée à rendre son site accessible pour le début de l'année 2009. Le 8 octobre 2010 une loi fédérale [3] a été promulguée qui oblige les constructeurs de téléphones mobiles et les diffuseurs de vidéos sur Internet à faciliter l'accès de leurs applications aux malentendants. et aux malvoyants.

Au cours de son audition, M. Dominique Berger a estimé que le jeu de la concurrence amènerait naturellement les constructeurs de produits informatiques à mieux prendre en compte les problèmes d'accessibilité.

Cependant, des actions plus volontaristes sont possibles, portant notamment sur la formation des ingénieurs en électronique. Sur le modèle de l'article 41 de la loi du 11 février 2005 [4] qui prévoit, dans la formation des architectes, un enseignement obligatoire sur l'accessibilité des personnes handicapées au cadre bâti, il conviendrait d'imposer, dans la formation des ingénieurs en informatique, un enseignement obligatoire relatif à l'accessibilité numérique.

Orientation n° 51 : rendre Internet plus accessible aux personnes handicapées

– Organiser une campagne d'information en direction des créateurs de sites Internet pour les sensibiliser aux problèmes de l'accessibilité numérique pour les personnes handicapées ;

– rendre obligatoire dans la formation des ingénieurs en informatique un enseignement relatif à l'accessibilité numérique pour les personnes handicapées, à l'instar de ce qui existe pour la formation des architectes.

(1) Le World Wide Web Consortium (W3C) est un organisme de standardisation à but non-lucratif.

(2) Cf. Communication de la Commission au Parlement européen « Vers une société de l'information accessible », Com (2008) 804.

(3) 21st century Communications and Video Accessibility Act.

(4) Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées.

V. DES MOYENS POUR RÉDUIRE LE FOSSÉ GÉNÉRATIONNEL

Comme il a été souligné précédemment, c'est l'âge, toujours, qui génère les principaux écarts : les plus jeunes sont quasiment tous internautes (99 %), alors que seule une personne sur cinq, passé 70 ans, se range dans cette catégorie.

Familiariser les personnes âgées aux outils numériques par un accompagnement personnalisé et des logiciels, voire des matériels, adaptés leur permettrait de correspondre plus aisément avec leurs proches, de bénéficier d'un suivi médical à distance, et ainsi de rester chez elles plus longtemps.

À partir de 55 ans, l'accès à un ordinateur ou à Internet diminue progressivement, presque linéairement, avec l'âge. Les seniors en France paraissent plus isolés que dans certains autres pays, qui ont su mieux les préparer à l'utilisation d'Internet en leur permettant d'accéder à des centres de formation ou en adaptant l'ergonomie des ordinateurs.

Les maisons de retraite et les accueils de jour pourraient comporter des espaces numériques adaptés permettant non seulement aux personnes âgées de correspondre avec leurs proches, mais aussi de les assister, par exemple celles souffrant de la maladie d'Alzheimer, dans le maintien d'une activité intellectuelle et sociale.

Aux Pays-Bas, le projet *SeniorWeb* a ainsi été conçu pour lutter contre l'isolement des personnes âgées, renforcer leur autonomie et améliorer leur qualité de vie. Il a conduit à la création d'une communauté virtuelle qui propose à ses membres des cours ou des jeux en ligne, des forums et des groupes de discussion. Cinquante-cinq mille personnes âgées suivent ces cours annuellement. Plusieurs milliers de volontaires répartis dans 375 centres dédiés dispensent aux personnes âgées des cours adaptés et peu onéreux et fournissent même une aide à domicile aux personnes qui le souhaitent.

Le développement des espaces numériques de travail peut contribuer à permettre aux personnes âgées de se familiariser avec les outils numériques et les campagnes d'information dont la mission préconise le développement pourraient sensibiliser les personnes âgées aux bénéfices que pourraient leur apporter les technologies numériques.

Une autre piste intéressante, qui pourrait être encouragée, serait d'organiser un accompagnement des personnes âgées dans l'apprentissage d'Internet à domicile (utilisation de la messagerie électronique, aide au remplissage de formulaires électroniques…) par les jeunes en service civique à travers des visites et un contact qui seraient un moyen intéressant de recréer un lien intergénérationnel.

Orientation n° 52 : réduire le fossé générationnel

– installer des espaces numériques dans les maisons de retraite et les accueils de jour ;

– organiser un accompagnement des personnes âgées dans l'apprentissage d'Internet à domicile (utilisation de la messagerie électronique, aide au remplissage de formulaires électroniques…) par les jeunes en service civique.

TITRE QUATRIÈME

QUELLE GOUVERNANCE

AU SERVICE DE CES DROITS ?

La gouvernance de l'Internet pose des difficultés particulières résultant de ce que le réseau des réseaux constitue un nouvel espace international qui transcende les frontières, un espace décentralisé qu'aucun opérateur ni aucun État ne maîtrisent entièrement, un espace hétérogène, à la fois lieu de communication, d'expression et de création, mais aussi lieu de travail, de commerce, de pouvoir...

Ensemble de réseaux informatiques privés et publics interconnectés grâce au protocole de communication commun, *TCP/IP (Transmission Control Protocol/Internet Protocol)*, Internet repose sur le principe d'une architecture décentralisée, dépourvue d'autorité centrale, ce qui lui a permis d'évoluer de façon autonome. C'est pourquoi, il est encore perçu par de nombreux internautes comme un espace de liberté totale, capable de se réguler tout seul et dans lequel toute velléité d'intervention des États est regardée avec méfiance.

L'autorégulation, qui repose sur l'idée selon laquelle il reviendrait aux acteurs économiques, conscients du fait que leur rentabilité économique repose *in fine* sur la confiance des utilisateurs, de s'imposer des codes et des règles de bonne conduite, doit certes jouer un rôle mais ne saurait satisfaire tous les besoins de régulation engendrés par le développement des usages d'Internet (demande de sécurité vis-à-vis des contenus illégaux, de protection de la vie privée et des données à caractère personnel, de sécurité dans le commerce en ligne, de protection des droits de la propriété intellectuelle, de garantie de la neutralité de l'Internet etc.)

Cependant, le caractère spécifique et novateur de l'Internet interdisant la transposition pure et simple des dispositifs de régulation étatique qui ont pu être mis en place dans les secteurs de l'audiovisuel et des télécommunications, les pouvoirs publics ont mis en place une forme nouvelle et originale de régulation, associant acteurs publics et privés : la corégulation. Cette dernière était jusqu'à présent exercée dans le cadre du Forum des droits sur Internet, espace de rencontre entre la régulation publique et l'autorégulation, auquel est venu succéder, le 27 avril 2011, un Conseil national du numérique.

Enfin, compte tenu des limites inhérentes à toute initiative purement nationale dans un espace déterritorialisé et largement dominé par l'initiative privée, la coopération internationale des États est indispensable pour faire faire du Web un espace de « civilité mondiale ».

I. LES ENJEUX NATIONAUX DE LA RÉGULATION

A. LE DÉBAT SUR L'ARTICULATION ENTRE LES DIVERSES AUTORITÉS PARTICIPANT À LA RÉGULATION D'INTERNET

1. Une multiplicité de régulateurs n'ayant pas été créés spécifiquement pour réguler l'Internet

En France, on doit constater qu'une multiplicité d'acteurs (CSA, ARCEP, CNIL, Autorité de la concurrence, HADOPI) participe à la régulation de l'Internet sans qu'aucune régulation globale, et, pour tout dire, totalement efficace ne soit assurée par aucun de ces acteurs.

Indiquons le d'emblée, aucune autorité n'est ici en cause spécifiquement car aucune n'a été créée pour réguler l'univers très particulier d'Internet dont les acteurs majeurs ne sont au demeurant pas situés en France.

Le CSA est compétent sur les programmes de télévision ou de radio diffusés par Internet, mais pas sur les sites Internet eux-mêmes. La loi du 5 mars 2009 relative à la communication audiovisuelle et au nouveau service public de la télévision a par ailleurs étendu sa compétence aux services de médias audiovisuels à la demande mais les contenus audiovisuels sur le net dépassent largement le champ de la régulation effectuée par le CSA. Les systèmes de protection mis en place pour réguler les médias traditionnels que sont la radio et la télévision sont en effet difficilement transposables aux nouveaux supports de diffusion.

S'agissant du rôle à attribuer au CSA, lors de la table ronde sur la protection de l'enfance sur Internet organisée par la mission le 9 novembre 2010, Mme Justine Atlan, directrice de l'association e-enfance, a estimé que l'élargissement de ses compétences à Internet était infondé puisqu'il ne s'agit pas du même média et qu'un Conseil national du numérique serait mieux à même de réguler Internet.

S'agissant de la CNIL, M. Jean-Emmanuel Ray, spécialiste du droit du travail et des TIC et professeur à l'Université Paris I-Sorbonne, a estimé que sa configuration initiale n'était pas opérationnelle dans l'univers numérique, en rappelant qu'elle a été créée pour contrôler l'État, et non pas *Google* et *Facebook*.

Quant à l'ARCEP, elle a été créée pour accompagner la fin du monopole de l'État dans le domaine des télécommunications et a aujourd'hui compétence sur les seules questions relatives à l'infrastructure de l'Internet.

Aucune de ces autorités n'a donc une vocation naturelle à réguler l'univers de l'Internet.

2. Le débat sur l'opportunité d'une « rationalisation » entre ces divers acteurs

La question de la convergence et du rapprochement entre le CSA et l'ARCEP est régulièrement évoquée, alors que plusieurs autres pays disposent d'une seule et même autorité pour exercer leurs compétences.

La Commission pour la libération de la croissance française, dite « commission Attali », dans son rapport rendu en janvier 2008, avait d'ailleurs préconisé de coordonner l'ARCEP et le CSA. Pour elle « *La convergence entre téléphonie fixe et mobile, télévision et accès à Internet est devenue aujourd'hui une réalité. Elle concerne aussi bien les réseaux que les terminaux ou les services. Internet a permis l'éclosion d'offres* triple–play *ou* quadruple–play. *La vidéo à la demande se développe. Le très haut débit renforcera encore cette convergence, qui pousse les entreprises à s'intégrer verticalement afin de proposer au client final des bouquets de services attractifs, relevant aussi bien de la communication audiovisuelle que des communications électroniques.*

L'exigence de mobilité crée également une demande plus forte d'accès au spectre hertzien pour des usages extrêmement variés (téléphonie, télévision mobile personnelle, etc.). Pourtant, l'organisation de la régulation reste marquée en France par une séparation « verticale » entre l'univers audiovisuel régulé par le CSA, aussi bien en ce qui concerne les réseaux (fréquences de diffusion) que les contenus (radio, télévision) et le monde des communications électroniques dont les règles relèvent entièrement de l'ARCEP. La révolution numérique appelle pourtant des arbitrages procédant d'une vision d'ensemble, notamment en ce qui concerne la gestion et l'attribution des ressources hertziennes aux différents opérateurs.

Le renforcement de l'efficacité de la régulation peut trouver deux types de réponse : soit un rapprochement institutionnel sur les modèles américain, britannique ou italien, soit, plus efficacement, une meilleure articulation des responsabilités de chacun des régulateurs en distinguant plus clairement leurs fonctions : la régulation éthique des contenus, confiée au CSA ; la régulation économique et technique des supports, relevant de l'ARCEP. »

Le rapport du comité d'évaluation et de contrôle des politiques publiques (CEC) présenté en octobre 2010 par MM. René Dosière et Christian Vanneste, propose la fusion de l'ARCEP, du CSA et de l'HADOPI. Quant à M. Éric Besson, ministre de l'Industrie, de l'énergie et de l'économie numérique, il a proposé un rapprochement entre l'ARCEP, le CSA et l'Agence nationale des fréquences.

Le phénomène de convergence numérique bouscule les secteurs de l'audiovisuel et des communications électroniques, les sociétés de télévision étant de plus en plus concurrencées par les opérateurs de télécommunications.

Selon les rapporteurs du CEC, « *la convergence numérique pose le problème de la despécialisation des réseaux (usages audiovisuels ou*

communications électroniques) et du dividende numérique (revendication des fréquences laissées par les chaînes audiovisuelles à la suite de l'abandon de la TNT). Le passage au numérique, avec la multiplication des possibilités d'émettre (Internet, téléphonie mobile…), bouscule le mode de régulation du CSA fondé sur l'attribution gratuite de ressources rares (fréquences) en contrepartie d'obligations (quotas…). »

Les rapporteurs du CEC soulignent en outre que « *la convergence numérique entraîne un besoin d'expertise accru du CSA en technologies numériques. Une synergie pourrait intervenir avec les ingénieurs au service de l'ARCEP. Une mise en commun des services techniques permettrait une meilleure maîtrise de la technologie. Une mise en commun des moyens de recherche et développement accroîtrait les compétences en matière de régulation technique et économique (concurrence). Bien sûr la mise en commun des fonctions support engendrerait des économies.* »

Enfin, les rapporteurs du CEC s'interrogent sur la justification de l'existence de la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI). Il s'agit, selon eux, une fois de plus d'une réponse ponctuelle à un problème spécifique. « *Certes la création d'une nouvelle autorité indépendante chargée de surveiller le respect des droits et de lutter contre le piratage jouit d'une visibilité maximale pour les auteurs. Mais on peut se demander pourquoi l'ARCEP, chargée de réguler les communications électroniques, dont fait partie l'Internet, ne pourrait pas en être chargée.* »

M. Jean-Ludovic Silicani, lors de son audition du 30 juin 2010, a jugé excellente la coopération entre ces deux autorités tout en rappelant que la législation consacrait l'existence de deux métiers bien distincts : d'une part, s'assurer du respect des obligations en matière de création et de pluralisme audiovisuels (CSA) et, d'autre part, veiller à la régulation économique des marchés et des réseaux (ARCEP). Ces deux métiers justifient l'existence de deux autorités, qui se parlent et échangent régulièrement. À cet égard, M. Jean-Ludovic Silicani a reconnu que les relations entre l'ARCEP et le CSA gagneraient à être approfondies. Toutefois, la fusion de ces deux autorités ne peut être réellement envisagée que si le cadre législatif de la régulation des télécoms et de l'audiovisuel était profondément bouleversé.

Sur l'opportunité d'un rapprochement ou d'une éventuelle fusion avec l'ARCEP, M. Michel Boyon, président du CSA, auditionné le 19 mai 2010 a estimé qu'il s'agissait « d'un faux ou plutôt d'un non-problème ». Les missions de l'ARCEP sont selon lui totalement différentes de celles du CSA. L'ARCEP a été créée pour accompagner la fin du monopole de l'État dans le domaine des télécommunications. Tandis que l'ARCEP attribue de « grands blocs de fréquences » à un opérateur qui paie pour les utiliser et les organise comme il veut, le CSA les attribue une par une à un opérateur déterminé pour un programme déterminé. Cette attribution est gratuite et la contrepartie de cette gratuité est constituée d'obligations (culturelles, en matière de contrôle du temps de parole des

personnalités politiques, de diversité et d'accessibilité des programmes. Les champs de compétences des deux autorités ne se chevauchent absolument pas. Cette situation n'empêche ni la coordination ni l'écoute, notamment sur des sujets comme l'utilisation du dividende numérique ou la télévision mobile personnelle. Les exemples étrangers d'un organisme unique sont souvent cités. Pourtant, là où il y a une institution unique, cette dernière est souvent quasi exclusivement consacrée aux télécoms parce qu'il s'agit de pays où il n'y a pas de contrôle des contenus. En outre, M. Michel Boyon a indiqué que là où il y a une institution unique qui s'occupait à la fois des contenus et des télécoms, on retrouvait à l'intérieur des services, des collèges et d'une bi-présidence la distinction nette entre les deux missions. Seule l'Italie fait figure de contre-exemple mais, dans ce pays, seul le Président s'occupe à la fois de contenus et de télécoms, le reste des services étant clairement scindé entre les deux missions.

Orientation n° 53 : assurer une plus grande coordination et renforcer le dialogue entre les différents régulateurs concernés par la régulation de l'Internet

La mission estime qu'un rapprochement et une plus grande coordination entre ces diverses entités sont indispensables. S'agissant par exemple d'un sujet comme la neutralité de l'Internet, il est évident qu'il ne saurait être l'affaire du seul régulateur sectoriel en charge des « tuyaux », c'est-à-dire l'ARCEP. Le régulateur ayant compétence sur les contenus, à savoir le CSA, mais également la CNIL et l'autorité de la concurrence ont également un rôle à jouer. De même, le développement des téléviseurs connectés devrait inévitablement amener les régulateurs à coordonner leurs efforts.

Concernant la régulation d'Internet, M. Emmanuel Forest, vice-président, directeur général délégué de Bouygues Télécom, entendu le 8 juin 2010, a estimé que ne constituait pas une faiblesse le fait que diverses autorités indépendantes et administrations centrales en soient aujourd'hui chargées en France. Créer une entité plus large qui coordonnerait les actions des divers organismes existants (ARCEP, CSA ou Autorité de la concurrence) n'aurait pas d'utilité. Concevoir une nouvelle structure qui reprendrait les compétences de toutes les autres ne paraît pas réaliste. Un tel projet ne correspondrait pas, non plus, à l'esprit de l'Internet qui consiste à faire travailler une multiplicité d'acteurs dans tous les domaines, à travers la corégulation.

La France disposait, avec le Forum des droits sur Internet (FDI), d'une telle instance indépendante de corégulation de l'Internet, capable de faire travailler ensemble une multiplicité d'acteurs sur toutes les questions posées par le développement d'Internet mais la mission constate avec regret qu'il lui a été substitué un nouvel organe, le Conseil national du numérique (CNN), dont les compétences sont limitées et dont on peut se demander si sa composition est objectivement la plus favorable à la protection des droits de l'individu dans l'univers numérique.

B. LA NÉCESSITÉ DE DISPOSER D'UNE STRUCTURE FORTE DE CORÉGULATION

1. Du Forum des droits sur Internet au Conseil national du numérique

Le 7 décembre 2010, dix ans après sa création, le Forum des droits sur l'Internet a été contraint de voter la dissolution anticipée de son association, les pouvoirs publics ayant décidé d'interrompre la subvention qui lui était accordée à la fin du mois de décembre 2010.

L'idée de créer un organisme spécifique pour réfléchir aux diverses questions juridiques posées par l'Internet apparaît pour la première fois dans le rapport du Conseil d'État de 1998, intitulé *Internet et les réseaux numériques*. Elle a été ensuite expertisée, à la demande du Premier ministre, par notre collègue Christian Paul dans son rapport de juillet 2000, *Du droit et des libertés sur Internet*, où il en confirme la pertinence et utilise pour la première fois le terme de « Forum ».

Le Premier ministre décide alors de lancer le projet du Forum des droits sur l'Internet, en décembre 2000, et d'en confier la responsabilité à Mme Isabelle Falque-Pierrotin, maître des requêtes au Conseil d'État. Fruit d'une réflexion collective, prenant acte de l'interdépendance des acteurs publics et privés sur le réseau et de l'évolution rapide des technologies, Le Forum est un lieu permanent de dialogue et de réflexion visant au développement harmonieux des règles et usages de ce nouvel espace. Il participe à la corégulation de l'Internet, sorte de troisième voie innovante entre l'autorégulation des acteurs privés et la régulation par les divers acteurs publics.

Organisé autour de quatre missions (la concertation, l'information et la sensibilisation, la médiation et la coopération internationale), le Forum associait, dans une structure de gouvernance innovante, représentants de l'État, du secteur privé et de la société civile. Son domaine de compétence couvrait l'ensemble des aspects de politique publique liés au développement de la société numérique sur le plan des contenus et des usages. Sans être un organe de supervision, et dépourvu d'une capacité de décision en propre, le Forum assumait cependant un rôle de facilitation, en liaison étroite avec les autorités publiques en particulier. Il agissait de sa propre initiative ou à la demande des autorités publiques ou d'autres acteurs, selon les modalités prévues dans sa charte.

Auditionnée par la mission le 2 juin 2010, Mme Isabelle Falque-Pierrotin, présidente du Forum des droits sur l'Internet (FDI), a d'abord dressé le bilan des actions menées par son association. Le FDI a été créé en 2001 à partir du constat qu'Internet n'était pas un nouveau média mais un nouvel espace de société qu'il convenait de réguler avec la participation de l'ensemble des intéressés (les autorités publiques, les acteurs économiques et la société civile), chacun avec leurs techniques propres d'intervention (la loi et le règlement pour l'État,

l'autorégulation pour le secteur privé, les initiatives individuelles pour la société civile). Ce dispositif a bien fonctionné. La capacité d'expertise du FDI, mobilisable tant par le Gouvernement que par le Parlement, s'est traduite par le traitement de plus de trente problématiques (le commerce électronique, la propriété intellectuelle, la protection de l'enfance, etc.) conduisant à des plans d'action définis et acceptés par toutes les parties prenantes. Le FDI s'est, par exemple, attaché récemment à la question du racisme sur Internet ; des recommandations ont été élaborées, dont le Premier ministre, M. François Fillon, a demandé la mise en œuvre.

En dix ans, le Forum des droits sur l'Internet a contribué à « construire la civilité de l'Internet », en faisant en sorte que le réseau ne constitue pas un espace de non droit, en recommandant des bonnes pratiques et en permettant aux Français de connaître les « nouvelles » règles d'usages de cet espace en construction. Plus précisément, le Forum des droits sur l'Internet a, depuis 2001, émis 34 recommandations sur des sujets très divers ; élaboré, pour le grand public, une large collection de guides et de fiches pratiques. En outre, sa plate-forme de médiation en ligne, mise en place en 2004, a traité près de 13 000 différends ; le service d'information a répondu à plus de 25 000 questions des internautes.

Lors de son audition, Mme Falque-Pierrotin a également exposé les raisons justifiant la création d'un Conseil national du numérique (CNN). Ce projet, qui était alors encore en suspens, a été initié par M. Éric Besson dans le cadre du plan France numérique 2012. Il répond à un changement d'échelle des enjeux de l'Internet qui compte aujourd'hui plus de trente millions d'internautes en France et pose de nouvelles questions.

Face à cette évolution, quatre raisons pouvaient, selon Mme Falque-Pierrotin, être avancées pour expliquer la nécessité de mettre en place un Conseil national du numérique.

La première raison est que la société civile, pourtant très présente sur le réseau, n'a pas été assez écoutée. Celle-ci recherche en priorité à sécuriser l'utilisation d'Internet et connaît mal les conditions dans lesquelles se font les échanges en ligne. Elle a besoin d'un garant sous la forme d'un pôle clairement identifié.

La deuxième raison est que le dispositif public s'est, certes, renforcé en engageant des réflexions sur les problèmes posés par l'Internet mais s'est aussi émietté en multipliant les organismes, notamment les autorités administratives indépendantes. Une multiplicité de guichets est ainsi proposée aux acteurs du numérique sans qu'il y ait de vision partagée. Il est temps de resserrer cette organisation.

La troisième raison est que les besoins de régulation se sont affinés. En 2001, l'enjeu était de réfléchir au cadre juridique adéquat. Aujourd'hui, il nous faut descendre dans la « granularité », dans la « finesse » des usages de l'Internet.

La loi est, en effet, mal à l'aise face aux diverses utilisations faites du Web et court le risque de devenir rapidement obsolète. Il est clair, par exemple, que la régulation de la publicité passe par le recours à des outils plus souples que la loi, de nouvelles formes de publicité non visées par la réglementation pouvant toujours apparaître.

Mme Falque-Pierrotin a souligné que la mise en place de *chartes* répond à cette préoccupation. Cette technique de régulation est particulièrement intéressante, sous réserve que les engagements pris soient contraignants et ne se réduisent pas à une opération de communication. À cette fin, il faut un « lieu » qui gère ce type de rapport entre le public et le privé. Selon la présidente du FDI, mesurer dans le temps le respect des engagements contractuels pris par des acteurs privés est une approche nouvelle que le CNN sera à même d'engager. Celui-ci pourra, par exemple, suivre l'application de la future charte portant sur le droit à l'oubli.

Enfin, la quatrième raison justifiant la création du CNN tient au caractère international des enjeux de l'Internet. Il faut mobiliser les acteurs publics et privés pour défendre des objectifs communs face au développement de grands opérateurs économiques tels que *Google* ou *Facebook*. Le CNN sera le lieu où pourra se nouer ce dialogue. Une telle démarche n'aura d'effectivité que si la société civile et le secteur privé y sont impliqués. Le CNN sera ainsi un outil, certes atypique, mais très précieux pour faciliter la prise de décision des autorités publiques.

Alors que le besoin de régulation d'Internet va croissant, l'objectif semblait donc être de bâtir une nouvelle structure plus ambitieuse et plus large autour du Forum des droits sur Internet reprenant à tout le moins, et si possible en les approfondissant, l'ensemble de ses compétences.

2. Le Conseil national du numérique : une structure qui ne répond pas aux besoins de régulation de l'univers numérique

Structure programmée par le Plan France Numérique 2012 du 20 octobre 2008, la création du CNN était initialement prévue pour début 2009. Après deux ans d'attentes et à la suite de la remise, le 25 février 2011, par M. Pierre Kosciusko-Morizet, PDG et co-fondateur de Price Minister, d'un rapport commandé par le ministre de l'Industrie, M. Éric Besson, le CNN a enfin vu le jour le 27 avril 2011, avec une composition et des compétences qui ne correspondent pas aux ambitions et aux besoins exposés par Mme Isabelle Falque-Pierrotin lors de son audition par la mission.

a) Une composition hautement discutable

Le CNN compte 18 membres : Gilles Babinet (Musiwave, Eyeka, CaptainDash), son président, Patrick Bertrand (Cegid, Afdel), Jean-Baptiste Descroix-Vernier (Rentabiliweb), Giuseppe Di Martino (Dailymotion, ASIC), Frank Esser (SFR, FFT), Emmanuel Forest (Bouygues Télécom), Gabrielle

Gauthey (Alcatel-Lucent), Pierre Louette (Orange), Alexandre Malsch (Melty), Daniel Marhely (Deezer), François Momboisse (Fnac, Fevad), Xavier Niel (Iliad/Free, Kima Ventures), Jean-Pierre Remy (PagesJaunes), Marie-Laure Sauty de Chalon (AuFéminin), Marc Simoncini (Meetic, Jaina Capital), Jérôme Stioui (Ad4Screen), Bruno Vanryb (Avanquest Software, Syntec Numérique) et Nicolas Voisin (Owni).

Cette composition, plus proche de celle d'un syndicat d'industriels du numérique que d'un organe de corégulation associant l'ensemble des parties prenantes a de quoi surprendre puisque le CNN ne comporte, contrairement aux préconisations du rapport de M. Pierre Kosciusko-Morizet, d'associer largement la nation aux choix publics en matière d'Internet, aucun représentant de la société civile, des consommateurs, aucun parlementaire, mais seulement des industriels du numérique. Or, l'une des raisons justifiant de passer du FDI au CNN était pourtant que la société civile n'avait pas été suffisamment écoutée.

La composition du CNN fait ainsi l'objet de nombreuses critiques depuis sa mise en place.

Le président de l'association UFC-Que Choisir, M. Alain Bazot, a qualifié la nouvelle instance de « Medef du numérique » en regrettant qu'une « *belle brochette de stars de l'économie du numérique* » ne fasse pas la moindre place à un parlementaire et à un représentant des consommateurs [(1)].

Le Syndicat de la presse indépendante d'information en ligne (Spiil) s'est élevé contre le mode de nomination des membres (par le seul président de la République) qui n'offrirait pas de garantie suffisante sur son indépendance et va à l'encontre du rapport de M. Pierre Kosciusko-Morizet qui préconisait une instance composée « de personnes élues et non désignées » [(2)].

Le Spiil demande donc que la nomination et la composition du CNN soient totalement revues, afin que ce Conseil puisse inclure des représentants des citoyens, des utilisateurs, des éducateurs et, bien sûr, des professionnels de l'information, désignés par leurs pairs.

Le Groupement des éditeurs de services en ligne (GESTE) a indiqué qu'« *en donnant une telle primauté aux intermédiaires dans les futures décisions législatives, le Président prend le risque de renforcer encore leur poids sur un marché qu'ils dominent déjà outrageusement* (...) *L'étrange composition du CNN, offrant un tel poids à ces derniers dans des décisions politiques aussi majeures que la neutralité du net, afflige les éditeurs.* » [(3)]

La SACD (Société des auteurs et compositeurs dramatiques) et la SCAM (Société civile des auteurs multimédia) ont uni leurs voix pour dénoncer « *une*

(1) ZDNet France, 26 avril 2011.
(2) Ibid.
(3) Ibid.

composition qui ne permettra pas de mettre sur pied une instance réellement indépendante, pluraliste et représentative des enjeux qui traversent le numérique. » (1)

Enfin, pour M. Benoît Tabaka, secrétaire général de l'ASIC (association des services Internet communautaires), « *le champ d'action du conseil dépendra de ses membres, et il est évident que des industriels seront moins aptes à se saisir de questions d'éducation ou de santé numériques.* » (2)

b) Des missions très en retrait par rapport à celles du Forum des droits sur Internet

Selon la communication du Conseil des ministres, le Conseil national du numérique aura pour missions principales :

— d'émettre des avis, à la demande du Gouvernement, sur les projets législatifs et réglementaires pouvant avoir des conséquences sur l'économie numérique ;

— et de formuler des recommandations participant, à la fois, au développement de l'économie numérique elle-même et au développement de la réflexion prospective sur ce secteur.

Ainsi, conformément aux préconisations du rapport M. Pierre Kosciusko-Morizet, le CNN ne dispose d'aucune compétence de médiation des litiges entre acteurs du numérique, alors même que le service médiateur du net du Forum des droits sur l'Internet (FDI) venait d'être récompensé par le premier trophée de l'innovation en médiation de l'Association nationale des médiateurs…

Lors de son audition par la mission, le 2 mars 2011, M. Jean-Emmanuel Ray a estimé que la fonction de médiation qu'assurait le Forum des droits de l'Internet devait être maintenue, le monde numérique étant en effet un domaine mal encadré par les normes de droit où la médiation apparaît essentielle. En outre, il a souligné que le travail réalisé par Mme Isabelle Falque-Pierrotin en matière de médiation avait rendu des services considérables, même si l'œuvre accomplie était restée discrète et méconnue des médias.

De façon encore plus surprenante et inquiétante, l'élaboration et le contrôle de l'application de « chartes de bonne conduite » entre les acteurs du numérique ne font pas partie du périmètre de compétences du nouveau CNN, alors même qu'il s'agissait d'une fonction clé du FDI dont Mme Isabelle Falque-Pierrotin estimait qu'elle devait être particulièrement renforcée et que l'action nº 145 du Plan Économique Numérique préconisait la création d'un « conseil national du numérique » doté de plusieurs fonctions, dont « *une fonction de*

(1) Ibid.
(2) World e.gov Forum, 21 avril 2011.

concertation avec l'ensemble des acteurs du numérique conduisant, notamment, à l'élaboration de chartes d'engagements et de bonne conduite ».

Concernant le rôle du futur Conseil national du numérique, M. Daniel Kaplan, délégué général de la Fondation pour l'Internet nouvelle génération, auditionné par la mission le 13 avril 2011, a regretté la disparition du Forum des droits sur l'Internet qui avait été une expérience originale, éloignée des pratiques de régulation traditionnelles en France. Il avait souhaité que l'organisme qui devait le remplacer n'ait pas moins de pouvoir, conserve les mêmes fonctions de médiation et puisse continuer à diffuser des documents pédagogiques.

M. Jean-Marc Manach, journaliste spécialisé dans les technologies de l'information et de la communication, auditionné le 14 avril 2011, a estimé qu'il était peu probable, d'après les informations dont il disposait au moment de son audition sur les contours du futur CNN, que ce dernier ait la même efficacité que le Forum des droits sur Internet.

Orientation n° 54 : préconisations relatives au Conseil national du numérique

La mission déplore la disparition d'une structure de médiation et de régulation telle que le Forum des droits sur Internet. Elle appelle de ses vœux le retour à une composition plus représentative de l'ensemble des parties prenantes de l'univers numérique, notamment les représentants des ayants droit, des associations de consommateurs et plus largement de la société civile, et un modèle plus ambitieux d'enceinte de corégulation disposant de l'ensemble des compétences qui étaient celles du Forum des droits sur Internet, en particulier celle de médiation et d'élaboration et de suivi de chartes de bonnes conduites.

II. LE BESOIN DE CONVERGENCES INTERNATIONALES

Dans l'ensemble du présent rapport une évidence est apparue. La promotion et la protection des droits de l'individu dans l'univers numérique supposent naturellement d'intervenir au plan international. Comment peser, sinon, face à des groupes formidablement novateurs mais auxquels un poids financier considérable donne l'illusion de la toute puissance ? À l'arrogance de certains, il convient d'opposer le sens de la responsabilité des États au service des citoyens avec le souci de préserver Internet comme espace de liberté.

L'équilibre est difficile à atteindre. Les développements qui précèdent dans le présent rapport le montrent. Les débats qui se sont déroulés lors du e-G8 de mai dernier à Paris, ou en marge de celui-ci, en témoignent également.

Dans cette voie étroite qui consiste à maintenir la liberté dans le monde numérique et à protéger les individus et leurs droits, l'Europe peut être porteuse d'un message.

A. OUVRIR DES ESPACES DE CONCERTATION AU PLAN INTERNATIONAL

1. L'e-G8 de Paris ou comment poser les termes du débat au plan international

L'initiative prise par la France de mettre la question de l'Internet à l'ordre du jour du dernier G8 qui s'est tenu à Deauville en mai 2011 constitue une première. Afin de nourrir la réflexion des chefs d'État et de gouvernement de la France, de l'Allemagne, du Canada, des États-Unis, de l'Italie, du Japon, du Royaume-Uni et de la Russie, un e-G8 s'est tenu à Paris, réunissant les représentants des grands groupes du numérique mondiaux mais aussi des ingénieurs, des intellectuels, des journalistes, des blogueurs. Sur des sujets aussi variés que la contribution du numérique à la croissance, l'éducation, les *open data*, l'avenir de la presse, la vie privée [(1)]… ont été abordés. À l'issue de deux journées de travaux, une délégation de cet e-G8 s'est rendue à Deauville pour dialoguer avec les membres du G8.

Le message délivré par la délégation de l'e-G8 a été le suivant : « *La délégation a d'emblée souhaité rappeler aux leaders du G8 que l'Internet constitue un puissant vecteur d'épanouissement individuel, de libre expression et de développement personnel. Au niveau collectif, Internet est une force positive de changement, capable de renouveler la manière dont les groupes et les organisations coopèrent et agissent – force ayant reçu une confirmation spectaculaire à l'occasion du Printemps arabe. Du point de vue économique, l'Internet est un formidable créateur de richesses et d'emplois. Il est également à l'origine d'une reconfiguration profonde de la façon dont fonctionnent les économies modernes. La transformation par le numérique de tous les secteurs économiques s'accompagne de création nette d'emplois : pour un emploi supprimé, 2,6 emplois nouveaux sont créés. La délégation l'a souligné : il faut libérer les énergies prêtes, dans tous les secteurs de la société, à s'investir dans le numérique. Pour que ces bénéfices soient concrétisés, la délégation a souhaité inviter les leaders du G8 à des politiques actives d'investissement, ou de soutien ou d'encouragement aux investissements, afin de garantir l'accès de tous leurs citoyens à un Internet libre, rapide, et sécurisé. La délégation a pu faire part de l'existence de débats en matière de régulation, évoqués à l'occasion d'échanges sur la propriété intellectuelle, les logiciels, la protection de la vie privée et la cybercriminalité. Protéger, sans entraver : réguler, sans remettre en question la valeur de liberté qui se situe au fondement du développement de l'Internet. Tels sont les termes d'un débat que le premier e-G8 forum s'est efforcé de poser, et auquel il a donné une structuration indispensable. La délégation a également voulu souligner que la croissance exponentielle des flux d'informations, l'interconnexion croissante des réseaux, appelait de la part des pouvoirs publics une action en vue d'assurer la stabilité, la sécurité, et le développement des infrastructures matérielles sans lesquelles Internet n'existe pas*. »

(1) http://www.eg8forum.com/fr/

Sont exprimées dans ce communiqué final du e-G8 des préoccupations que la mission partage.

Même si on ne doit pas espérer que de telles déclarations aient des effets concrets et ce, d'autant plus que, lors de ce forum, les positions entre les différents intervenants n'ont pas été consensuelles, il ne faut pas regarder ces initiatives avec scepticisme. Il s'agit d'un premier pas qui en appelle d'autres.

Il est cependant important d'évoquer aussi les critiques qui ont accompagné l'organisation de cette réunion. On a vu des acteurs de la société civile constituer un « contre e-G8 » à la manière de ces contre-sommets qui ont été organisés ces dernières années pour contester ces réunions entre « grands » de ce monde.

Les critiques exprimées ont été de plusieurs ordres. Elles ont porté sur la composition de ce forum officiel, réunissant principalement, selon les contempteurs de cette manifestation, des représentants du *e-business*. D'autres voix ont également invoqué la volonté de main mise des États sur les réseaux aux fins de restreindre la liberté des internautes. La CNIL a pris part à ces critiques en regrettant, lors de l'ouverture de ce e-G8, l'absence de représentants des régulateurs et des associations de défense des libertés ou de consommateurs dans ce forum, alors même que certains sujets comme la vie privée les concernaient au plus près. Cependant, dans un communiqué diffusé à l'issue cette fois du G8, la CNIL s'est félicitée de la déclaration finale adoptée par les chefs d'États et de gouvernement qui place la question de la protection des données personnelles et de la vie privée au cœur de l'agenda international. Pour la CNIL, cette initiative doit désormais se traduire par l'élaboration d'un instrument juridique international.

En effet, dans leur déclaration finale, les chefs d'États et de gouvernements des pays du G8 réaffirment que la protection des données personnelles est un droit fondamental et un élément essentiel pour assurer la confiance des utilisateurs. Ils appellent même *« à la définition d'approches communes tenant compte des cadres juridiques nationaux, qui soient fondées sur les droits de l'homme et protègent les données à caractère personnel, tout en permettant les transferts légitimes de données »*.

2. Faute d'une perspective de régulation internationale à moyen terme, un objectif : la concertation sous l'œil des citoyens

Tout au long de ce rapport ont été présentées des pistes pour engager des actions concrètes au plan international, par exemple en matière de promotion de la liberté d'expression et de communication sur Internet.

Rappelons que, lors du Sommet mondial sur la société de l'information en 2003 et 2005, l'ensemble de la communauté internationale – plus de 180 États – a reconnu la pleine applicabilité à l'Internet de la Déclaration universelle des droits

de l'homme, en particulier de son article 19 relatif à la liberté d'expression et d'opinion. Internet y a, par ailleurs, été qualifié de « *ressource publique mondiale* ».

Dans cette lignée, on a vu que des perspectives d'action plus concrètes avaient été tracées lors de la réunion consacrée à « Internet et la liberté d'expression » qui rassemblait une soixantaine de participants, représentants de dix-sept gouvernements, d'ONG, d'entreprises et d'organisations internationales le 8 juillet 2010 au ministère des Affaires étrangères et européennes, à Paris.

La mise en place, au niveau international, d'un mécanisme d'observation en matière de liberté d'expression et d'opinion sur Internet semble utile car, en fédérant l'ensemble des initiatives prises dans ce sens, notamment par les acteurs de la société civile, il permettrait de constituer un groupe de pression suffisamment puissant pour interpeller les États qui manquent à leurs engagements. On a observé, dans le cas des révolutions arabes, l'intérêt de maintenir une telle pression. On peut également évoquer l'aide aux défenseurs des droits de l'homme et aux cyberdissidents, qui doivent bénéficier du même soutien que les autres victimes de répression politique.

Le constat que fait la mission est qu'il n'est pas sérieusement envisageable d'organiser une réelle régulation à moyen terme au plan international pour des raisons évidentes. C'est par des actions ponctuelles et concrètes et la constitution de lieux, plus ou moins formels, réels ou virtuels, de concertation accueillant tous les acteurs du monde numérique que pourront être posés des jalons utiles pour l'avenir.

La mission a la conviction que c'est par ces formes de concertation et par la pression que pourront exercer les citoyens que l'on amènera les grands groupes du numérique à des positions tout à fait respectueuses des droits des individus et les États les moins scrupuleux en la matière ne pourront pas éternellement s'abstraire de cette pression internationale.

B. LA VOCATION DE L'EUROPE

Dans ce contexte international, face à une conception américaine qui, sans être caricaturée, est très différente de celle qui y est la nôtre, l'Europe doit peser en défendant un point de vue équilibré qui fasse toute sa place à la régulation.

1. L'Union européenne en première ligne

C'est au travers des textes que l'Union européenne peut adopter ou d'initiatives moins normatives prises au plan européen que peut se traduire cette volonté de peser face aux grands groupes du monde numérique pour faire respecter les droits des individus.

a) La révision de la directive du 24 octobre 1995 sur la protection des données personnelles

En matière de protection des données, on a évoqué le cadre juridique communautaire riche est exigeant.

On ne reviendra pas, à cet égard, sur l'impact du paquet télécoms en cours de transposition. Le chantier qui s'ouvre désormais est celui de la révision de la directive du 24 octobre 1995 sur la protection des données personnelles aujourd'hui officiellement engagée ; l'Union européenne va évidemment devoir prendre position dans le débat dont nous avons énoncé les termes dans le titre II de ce rapport. La communication faite par la Commission européenne le 4 novembre 2010 qui appelle à « *Une approche globale de la protection des données à caractère personnel dans l'Union européenne* » va dans le bon sens. Cependant, lors du déplacement de la mission à Bruxelles en octobre 2010, il a clairement paru que des conceptions distinctes s'opposaient parmi les États membres sur ce sujet. Il importe que dans les mois qui viennent les autorités françaises pèsent, en lien avec leurs homologues allemands, pour maintenir un très fort degré d'exigence en faveur de la protection des données personnelles face à des conceptions en particulier anglo-saxonnes qui s'en montrent moins soucieuses. C'est le sens de la déclaration commune signée par notre mission et la commission d'enquête du *Bundestag* évoquée ci-après.

b) La définition de principes d'action ou de co-régulation

Au-delà de l'adoption de textes communautaires contraignants, d'autres pistes sont également à creuser pour coordonner les actions des autorités concernées dans les États membres. On pense évidemment au rôle du G29 qui doit demeurer central et disposer des moyens de fonctionner.

On a également évoqué la fixation d'un cadre européen définissant les conditions d'un partenariat acceptable avec les acteurs privés pour la numérisation du patrimoine ou l'adoption, au plan européen, des mesures susceptibles de rétablir des conditions de concurrence plus favorable entre la presse écrite et les agrégateurs de contenus tels que *Google*.

La question du développement de la co-régulation à l'échelle européenne pour mettre l'accent sur la priorité que constitue la protection de l'enfance sur Internet doit aussi être mentionnée.

2. La déclaration parlementaire franco-allemande du 19 janvier 2011

***a) La création concomitante d'une mission d'information à l'Assemblée nationale et d'une commission d'enquête au* Bundestag**

Le 5 mai 2010, le *Bundestag* a décidé la création d'une commission d'enquête (qui correspond en France à une mission d'information) consacrée à

« Internet et la société numérique » (*Kommission, internet und digitale Gesellschaft)*. Cette initiative a reçu l'accord unanime de tous les groupes politiques du *Bundestag*.

Il est tout à fait remarquable que les parlementaires allemands aient pris cette décision au moment même où la création d'une mission d'information commune à la commission des Lois et à la commission des Affaires culturelles était décidée à l'Assemblée nationale.

La commission allemande est composée de 34 membres :

— 17 parlementaires (6 CDU/CSU, 4 SPD, 3 FDP, 2 *die Linke*, 2 *die Grünen*) ;

— 17 experts (juristes, ingénieurs, journalistes et différents responsables de projets sur Internet).

La commission est présidée par M. Axel Fischer, membre du CDU/CSU, élu du *Land* de Karlsruhe.

Quatre groupes de travail ont été créés à l'intérieur de la commission d'enquête autour des thèmes suivants :

— les données personnelles ;

— la neutralité du Net ;

— les droits d'auteur ;

— l'éducation aux médias.

On voit qu'hormis les droits d'auteur qui n'entrent pas dans le champ de la présente mission, les thèmes abordés recoupent ceux qui ont préoccupé la présente mission.

b) Une initiative sans précédent : une déclaration parlementaire commune

C'est pourquoi, à l'initiative du Président et des deux rapporteurs de la mission, des contacts ont été pris avec les membres de la commission allemande et qu'il a été décidé d'organiser, le 19 janvier 2011, une visio-conférence entre Paris et Berlin – par voie numérique donc – pour débattre et adopter une déclaration commune. Le compte rendu de cette réunion et la déclaration figurent en annexe de ce rapport [(1)]. Cette dernière a été adressée au Président de la République et au Premier ministre ainsi qu'aux deux Commissaires européennes en charge de ces questions, Mme Viviane Reding, vice-présidente de la Commission chargée de la

(1) Cf. annexes n^os^ 1 et 2.

justice, des droits fondamentaux et de la citoyenneté, et Mme Nelly Kroes, vice-présidente de la Commission chargée de la stratégie numérique.

• Pour des initiatives gouvernementales franco-allemande dans le cadre de la révision de la directive de 1995

Les membres de la mission d'information française et de la commission d'enquête allemande ont considéré qu'il était indispensable que les assemblées et les gouvernements de nos deux pays se consacrent pleinement à ces questions, qu'ils participent activement au niveau européen aux travaux de révision de la directive européenne 95/46/CE, relative à la protection des données et que, dans ce cadre, ils se prononcent conjointement pour un renforcement des droits des citoyens en matière de protection des données.

La mission et la commission ont également indiqué qu'elles apprécieraient qu'en l'espèce, il soit également fait référence à la communauté de vues entre les assemblées des deux pays, telle qu'elle est formulée dans la déclaration du 19 janvier 2011.

• Chaque citoyen doit être mis en mesure de faire respecter ses droits sur Internet

La déclaration commune insiste notamment sur le fait que la numérisation de nombreux processus dans l'administration, la vie économique et la vie quotidienne des citoyens entraînait une multiplication des traitements de données, de même qu'un accroissement perpétuel des informations stockées. Il est aussi constaté que les citoyens s'interrogent de plus en plus souvent sur la manière dont ils vont pouvoir exercer effectivement leur droit à la libre disposition de leurs données personnelles (ou « droit à l'autodétermination informationnelle » dans les termes de la Loi fondamentale allemande). Les possibilités croissantes d'interconnexion entre de multiples bases de données, tant dans la sphère publique que privée, constituent, en outre, un risque potentiel pour la protection des droits de la personne. La déclaration du 19 janvier 2011 indique qu'il est donc impératif de renforcer les droits de l'individu, que chaque citoyen doit pouvoir exercer et faire respecter ses droits à être informé sur les données le concernant et à pouvoir effacer, bloquer ou contester ces données, et que ces droits doivent être facilement applicables et effectifs, y compris dans le cadre d'Internet.

• Associer des modes de régulation étatique et des engagements volontaires de la part des acteurs du numérique pour protéger les données

La déclaration parlementaire franco-allemande reconnaît également tout l'intérêt de modes de régulation non étatiques, en faisant référence aux engagements volontaires de la part des parties prenantes qui peuvent contribuer à rehausser le niveau de protection des données. Des solutions techniques peuvent également être mises en œuvre très en amont avec des technologies de protection préventive qui intègrent, dès la conception des matériels et logiciels, la question de la protection des données personnelles.

De même, les prescriptions légales relatives aux technologies de protection doivent être élaborées selon le principe de la neutralité technologique afin de garantir la protection des données au fur et à mesure de l'évolution technologique – y compris sans que le législateur ait à intervenir.

La définition d'objectifs de protection peut avoir tout son sens à cet égard. Des procédures comme l'attribution de labels de qualité peuvent donner une impulsion efficace et orienter le marché vers une meilleure protection des données.

• La protection des données personnelles et des droits sur Internet passe par les citoyens eux-mêmes, grâce à l'éducation et à la formation

Enfin, la déclaration du 19 janvier 2011 note que le puissant attrait qu'exerce Internet réside dans sa conception décentralisée, qui sollicite la participation des utilisateurs, notamment pour élaborer des contenus. Cette participation entraîne une responsabilité nouvelle des internautes vis-à-vis d'une utilisation prudente de leurs propres données, mais aussi des données personnelles relatives à des tiers. Il est nécessaire qu'ils soient sensibilisés aux risques potentiels et informés sur les mesures volontaires de protection qui sont utiles. Aucune protection efficace des données ne sera possible sans qu'y soient associés les individus concernés. Un travail d'explication et le nécessaire partage de la connaissance technique avec les usagers constituent, par conséquent, des objectifs majeurs dans toute politique de protection. Renforcer chez chaque individu la conscience qu'il faut protéger les données constitue également une priorité dans toute la société. Les enfants et les jeunes, en particulier, ont besoin d'être protégés. Il est donc indispensable de proposer aussi une formation spécifique sur ces questions à destination précisément des jeunes.

En tant qu'espace d'interconnexion global en constante expansion, Internet peut considérablement favoriser le développement d'une communauté mondiale. C'est le forum d'information et de communication le plus libre qui soit au monde. Mais cela signifie aussi que les législations nationales, comme également les réglementations européennes, ne peuvent à elles seules réussir à écarter les risques qui pèsent sur les droits de l'individu même si de telles dispositions, nationales et européennes, peuvent évidemment être nécessaires et efficaces pour protéger les citoyens en ce domaine.

En conclusion de cette déclaration, la commission d'enquête du *Bundestag* allemand et la mission d'information ont estimé toutes deux que l'élaboration d'instruments internationaux, allant au-delà du cadre européen, s'imposait afin de permettre de mieux faire respecter la protection des droits de la personne.

CONCLUSION

La conclusion de ce rapport ne peut être que provisoire car nous ne sommes qu'au début d'un processus qui connaîtra des développements que nous ne sommes pas encore en mesure d'imaginer aujourd'hui. C'est le propre d'une révolution ; c'est ce qui fait également le sel de ce que nous vivons actuellement.

Ce rapport s'efforce de tracer quelques lignes de force qui peuvent guider une action. Face à la labilité du monde dans lequel nous évoluons, l'énoncé de principes stables est essentiel, notamment pour les plus jeunes.

Loin de se conclure par un constat d'impuissance pour les États, on a entendu, au contraire, montrer qu'en raison même des bouleversements nés de la révolution numérique, les autorités publiques trouvaient une nouvelle légitimité à agir. Mais cette régulation du monde numérique ne peut se faire qu'au profit des individus et de l'exercice de leurs droits et surtout en ayant toujours à l'esprit le principe de liberté qui est consubstantiel à l'idée même d'Internet ; c'est pourquoi cette régulation ne peut être menée que si les citoyens sont eux-mêmes en situation de manifester leurs choix de manière éclairée et de les faire respecter. Ils doivent être des acteurs à part entière de cette régulation.

C'est donc en une nouvelle conjonction, heureuse, de l'action des autorités publiques, nationales et internationales, et des citoyens qu'il faut placer ses espoirs, conjonction désormais facilitée au moins techniquement par Internet. C'est sans doute la condition nécessaire pour que les droits de l'individu puissent demain pleinement s'épanouir dans l'univers numérique.

EXAMEN EN COMMISSION

La commission des Lois constitutionnelles, de la législation et de l'administration générale de la République et la commission des Affaires culturelles et de l'éducation procèdent à l'examen des conclusions du rapport de la mission d'information commune sur les droits de l'individu dans la révolution numérique, au cours de leur réunion conjointe du mercredi 22 juin 2011.

M. Marcel Rogemont. J'ai suivi de près les travaux de la mission d'information et je remercie le président pour le bon déroulement de ses travaux et les deux rapporteurs pour la qualité de leurs préconisations. Les auditions présentaient toutes un grand intérêt.

Nos échanges avec nos collègues allemands doivent nous permettre de saisir Bruxelles de questions qui ne sont aujourd'hui pas abordées.

Je retiens deux grands sujets : l'éducation au numérique, notamment dans le cadre de l'Éducation nationale, et la protection des personnes. J'observe que la liberté de l'Internet a pour corollaire l'asservissement à la fonction publicitaire. Les entreprises collectent une masse d'informations qui finit par intéresser d'autres entités que les entreprises, comme en témoignent quelques exemples étrangers. Cette question est traitée dans le rapport, mais je tiens à souligner que les puces *RFID* devraient être « à activer » et non « à désactiver ». De même, il faut quatre ou cinq manipulations pour désactiver un compte *Facebook*. Nous devons insister sur ces enjeux auprès de l'Union européenne.

M. Jean-Luc Pérat. On constate aujourd'hui que l'éducation aux médias est encore insuffisante. Il convient de mobiliser l'Éducation nationale sur cet enjeu, il faut éviter les « zones blanches » et renforcer la formation académique des enseignants.

M. Dominique Le Mènер. Je me joins aux félicitations adressées aux rapporteurs et je tiens à souligner les limites et les difficultés techniques que présentent les outils de limitation d'accès à Internet. A côté de la liberté et des droits, il doit y avoir un contrôle. Il faudrait pouvoir passer par un filtre qui pourrait être la CNIL.

M. Jean-Jacques Gaultier. Ce rapport est tout à fait d'actualité. Il convient aussi de s'interroger sur la télévision, compte tenu du développement des téléviseurs connectés à Internet. Il convient de relever le défi des contenus dérégulés ou des régulations qui varient fortement selon les sites. La protection de l'enfance à l'égard de la violence et de la pornographie doit être un souci majeur.

Mme Françoise de Panafieu. Le rapport contient de bonnes propositions. Il y a effectivement un décalage entre notre perception et celle de Bruxelles comme j'ai pu le constater lors de notre déplacement auprès des instances de l'Union européenne. L'Europe n'exprime pas cette préoccupation. Pourtant, il

faudrait une démarche européenne pour peser face aux États-Unis. Je suggère donc que le rapport soit traduit en anglais et envoyé aux différents parlements des pays européens afin de créer un réseau à cette échelle.

Mme Laure de La Raudière. Je me réjouis que l'Internet soit une préoccupation majeure de l'Assemblée nationale en 2011, votre rapport d'information, comme celui que j'ai présenté avec Corinne Ehrel au sein de la commission des Affaires économiques sur la neutralité de l'Internet et des réseaux, fournissent une base de réflexion commune importante sur cette question. Trois commissions de l'Assemblée auront donc contribué à l'élaboration de ces rapports transpartisans. Au-delà de ce travail, il importe de continuer à informer sur ce sujet, à destination du grand public. Je souhaiterais vous interroger sur votre réflexion sur le télétravail et les moyens de donner des droits aux individus qui s'y adonnent, qui constituent une attente forte de nos concitoyens.

Mme Corinne Ehrel. Je salue également la dimension transversale de votre travail sur le monde numérique, que résume votre volonté de faire « de l'univers numérique un lieu d'épanouissement des droits des individus ». Il est important de considérer le numérique et l'Internet comme une chance pour la démocratie et l'innovation dans ce domaine. Comme les précédents intervenants, je souhaite souligner la convergence de nos rapports sur un certain nombre de points, et notamment ceux présentés dans le titre troisième sur le droit à l'accès à Internet. Comme Laure de La Raudière et moi-même, vous relevez la nécessité de l'intervention du juge pour encadrer le blocage légal.

À cet égard, que pensez-vous de la polémique soulevée à la suite de l'avis rendu par le Conseil national du numérique sur le projet de décret pris pour l'application de l'article 18 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, qui recommande de conditionner toute mesure de blocage à l'appréciation et au contrôle préalable du juge afin qu'elle ne relève pas de la seule autorité administrative comme le rend possible le projet de décret ?

M. Christian Vanneste. L'étude du numérique présentée par le rapport est excellente. Elle me conduit à vous poser trois questions.

Internet est la langue d'Ésope de notre époque : il peut être la pire ou la meilleure des choses. C'est notamment la meilleure des choses dans le domaine de la liberté. Entre les lois n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI) et les lois n° 2009-669 du 12 juin 2009, favorisant la diffusion et la protection de la création sur Internet et n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet (dites lois « HADOPI »), j'ai pris la mesure de cette dimension essentielle de la liberté dans la pratique d'Internet. Mais un problème se pose, qui est justement celui de la liberté et de ses limites, celui du très grand nombre d'images et d'informations relatives à la violence ou à la pornographie. Ces dernières sont notamment accessibles à un très jeune public

et sont sans doute suivies d'effets dans la vie quotidienne. Les faits divers extrêmes dont les exemples existent sur Internet ne sont peut-être pas étrangers à ces pratiques. Je me demande si les propositions n^{os} 35 et 37 de votre rapport sont à la mesure de ce problème. Le contraste me semble fort entre le danger justement souligné d'Internet et ces propositions. Une étude est actuellement menée en Grande-Bretagne qui examine s'il ne serait préférable de changer les conditions d'accès à Internet, en inversant le principe du contrôle parental et prévoyant que certains domaines ne pourront être ouverts qu'avec la volonté qu'ils le soient. L'orientation n° 37 me semble également un peu faible dans sa volonté d'éduquer le public, les parents sont en effet souvent inconscients des informations susceptibles d'être diffusées sur Internet.

Comme Mme de La Raudière, je me félicite du caractère transpartisan de ces études sur le numérique. J'entendais citer l'intervention spécifique du Conseil supérieur de l'audiovisuel (CSA), de l'Autorité de régulation des communications électroniques et des postes (ARCEP) et pourquoi pas de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI). Or, le rapport également transpartisan que j'ai publié avec M. René Dosière proposait un regroupement de ces trois autorités administratives indépendantes, d'une part parce que je pense qu'il y en a effectivement trop, mais aussi parce que la convergence sur Internet va conduire à ce que les différences de leurs champs d'intervention tendent à s'estomper. Qu'en pensez-vous ?

L'Internet est en effet un magnifique outil qui peut permettre de développer la démocratie ; M. Patrick Bloche ne pense-t-il pas qu'il serait mieux adapté pour l'organisation des primaires que prévoit un des partis politiques de ce pays pour désigner son candidat à l'élection présidentielle ?

Mme Martine Martinel. La remarque de M. Vanneste sur l'organisation des primaires au sein du Parti socialiste ne me semble pas adaptée au débat sur le rapport d'information qui nous est présenté ce matin. Ayant participé à la mission, j'en félicite le président et les co-rapporteurs non seulement pour la qualité du rapport mais aussi pour celle des auditions, tant pour leur progression que pour le choix des intervenants. La formule de M. Serge Tisseron sur les âges auxquels on devrait accéder au numérique et à l'audiovisuel a fait mouche, elle a surpris ou séduit. Pouvez-vous la préciser ? Quelle suite peut être donnée aux préconisations en matière d'élargissement du Conseil national du numérique, par exemple, aux associations de consommateurs et aux ayants droit ? Enfin dans le domaine de l'éducation et de la formation, ne conviendrait-il pas que le ministre de l'Éducation nationale prévoie une véritable formation des enseignants et un temps spécifiquement consacré en classe à l'éducation numérique, les « semaines » du Centre de liaison de l'enseignement et des médias d'information (CLEMI), par exemple, restant trop sporadiques.

M. Didier Mathus. Je me joins aux éloges adressés à nos deux rapporteurs pour cet excellent travail, qui donne un aperçu assez complet sur les questions posées par la révolution numérique. Des tensions contradictoires sont à

l'œuvre dans le monde de l'Internet, entre une aspiration à la liberté et une démocratisation de l'information et une volonté de contrôle marchand de la plupart des contenus. La discussion des lois « HADOPI » n'a été qu'un des révélateurs de cette dernière tendance. Je trouve, à cet égard, scandaleuse la campagne financée sur fonds publics en faveur de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI). Un aspect, cependant, ne me semble pas totalement éclairé par le rapport, celui de la qualité de l'information. Internet a été une révolution majeure dans la chaîne de diffusion de l'information. La situation ancienne qui voyait un émetteur de l'information s'adressant à des récepteurs passifs a cédé la place à une information collaborative, étudiée d'ailleurs aujourd'hui par de nombreux universitaires. Dès lors se pose avec une acuité accrue la question de la fiabilité de l'information diffusée, pour laquelle personne n'a de réponse, sauf à faire confiance aux marchés, l'internaute étant amené à en déterminer par lui-même la qualité, dans un contexte parasité par l'énormité des flux. Qu'en pensez-vous ?

M. François Vannson. Je souhaite féliciter les auteurs de ce rapport, extrêmement fourni, pour sa qualité. Cela dit, on peut se demander dans quelle mesure les règles de déontologie journalistique sont toujours respectées sur Internet. Il existe, en effet, une forme de décalage entre la pratique des médias traditionnels, que ce soit la presse écrite, les médias audiovisuels, etc. très attachés à ces règles, et celle qui prévaut s'agissant d'Internet. De manière à améliorer cette situation, ne pourrait-on pas envisager de s'appuyer sur l'histoire et les usages des autres médias ?

M. Patrice Verchère, rapporteur. Concernant l'éducation, l'orientation n° 36 rappelle que des efforts sont à faire en direction non seulement des enfants mais aussi des enseignants. On connaît les insuffisances du B2i. Nous estimons que l'Éducation nationale doit mettre en place de véritables cours consacrés à l'usage d'Internet car celui-ci est devenu un outil au même titre que l'anglais ou les mathématiques.

Le problème se pose aussi pour les adultes, bien souvent dépassés par l'évolution de la technologie.

Si la règle des 3 / 6 / 9 / 12 nous a séduits, c'est qu'elle est simple et facile à identifier par les parents. Il n'est évidemment pas question d'en faire une loi, mais elle donne des orientations dont les parents peuvent s'inspirer dans les responsabilités éducatives qui sont les leurs.

Quant à la déontologie des médias sur Internet, si la presse traditionnelle et professionnelle est bien présente sur le Net, il est de fait qu'on y trouve aussi un très grand nombre d'articles venant d'autres sources ; face à une telle masse d'informations, il paraît très difficile d'imposer des règles de déontologie.

M. Patrick Bloche, rapporteur. Nous avons voulu dans ce rapport donner une vision positive et optimiste d'Internet, qui est un outil aux potentialités

extraordinaires, sans être pour autant naïfs. Nous avons parfaitement conscience que cette architecture horizontale suscitant de la création à sa périphérie, ce média pluraliste et démocratique, cet Internet libre et ouvert tel qu'il était à ses débuts sur les campus américains il y a deux décennies, a aujourd'hui changé : il est de moins en moins gratuit et, parfois, de moins en moins libre. C'est pourquoi notre rapport rappelle la nécessité de protéger un Internet non marchand qui permette l'accès à l'information et à la culture.

En réaffirmant la liberté de communication sur Internet nous n'avons d'ailleurs fait que rappeler la décision du Conseil Constitutionnel du 10 juin 2009.

Dans le secteur des médias sur Internet, il est clair que la masse des informations diffusées sur le Net rend d'autant plus important le rôle des journalistes professionnels pour sélectionner ces contenus, les hiérarchiser et en donner la lecture la plus dynamique possible. Ainsi quand *Wikileaks*, dont le créateur, Julian Assange, a fait l'objet de tant de polémiques - on a même envisagé d'interdire l'hébergement de son site en France – a mis en ligne un très grand nombre d'informations, celles-ci ont encore dû être triées, mises en ordre et référencées dans le temps pour prendre un sens. C'est un grand quotidien du soir qui a fait ce travail indispensable.

Au sujet des puces *RFID*, le droit au silence des puces a fait l'objet d'un engagement très fort de l'Europe qui passe en particulier par la prise en compte de la vie privée dès la conception des technologies – ce qu'on appelle le « *privacy by design* ».

En ce qui concerne le rôle de l'Éducation nationale dans l'apprentissage d'Internet, il se pose clairement un problème de moyens. Dans notre rapport, nous proposons qu'une semaine soit consacrée à l'éducation aux nouveaux médias dans le cadre de la formation des enseignants. Nous citons aussi la loi du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communication électronique : « *Dans le cadre de l'enseignement d'éducation civique, les élèves sont formés afin de développer une attitude critique et réfléchie vis-à-vis de l'information disponible et d'acquérir un comportement responsable dans l'utilisation des outils interactifs, lors de leur usage des services de communication au public en ligne. Ils sont informés des moyens de maîtriser leur image publique, des dangers de l'exposition de soi et d'autrui, des droits d'opposition, de suppression, d'accès et de rectification prévus par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.* »

Nous avons aussi repris une proposition faite par la Ligue de l'enseignement de créer un B2i pour les adultes afin de promouvoir un usage responsable d'Internet.

De façon générale, notre rapport a été plus orienté vers la question des réseaux sociaux et de leur utilisation par les jeunes que vers celle des contenus

violents et pédopornographiques contre lesquels luttent avec une très grande efficacité la police et la gendarmerie.

M. Christian Vanneste a soulevé la question de la fusion du CSA et de l'ARCEP, sujet qu'il avait abordé, avec M. René Dosière, dans un rapport du Comité d'évaluation et de contrôle. Notre orientation n° 53 ne va pas si loin mais en appelle à un regroupement, que l'émergence des télévisions connectées imposera tôt ou tard.

Cette convergence de positions, au-delà des partis, et que Mme Corinne Erhel et Mme Laure de La Raudière ont également évoquée dans leur rapport, pourrait être l'occasion de prendre en commun des initiatives législatives pertinentes.

Nous avons pris acte de l'avis du CNN sur le projet de décret d'application de l'article 18 de la loi pour la confiance dans l'économie numérique. Si nous sommes, par ailleurs, favorables à un CNN plus ouvert, son avis réaffirmant la nécessité de recourir au juge pour toute mesure de blocage correspond à l'idée formulée, en particulier, dans notre rapport.

Enfin, je reviendrai sur la déception que nous a causée notre voyage à Bruxelles. Les préoccupations françaises portant sur la protection de la vie privée y trouvent un écho limité ; nous nous attendions à des positions plus ouvertes en faveur d'une régulation, au bon sens du terme, visant à responsabiliser les acteurs. Mais la ligne suivie consiste plutôt à faire confiance dans le marché et à n'admettre qu'une régulation par les opérateurs sans faire appel à la puissance publique et à l'intérêt général.

M. Patrice Verchère, rapporteur. La question de l'usage de l'ordinateur comme outil de travail est abordée dans le rapport : on propose des mesures pour que les internautes, dans certaines conditions, ne soient pas dépossédés de leur ordinateur personnel ; on suggère aussi des connexions haut débit à faible coût pour les plus démunis qui se lancent dans des activités de télétravail. Enfin, on propose même un droit à la déconnexion pour éviter le travail en continu, selon une préconisation du professeur Jean-Emmanuel Ray.

La masse d'informations exploitées sur Internet est telle qu'on peut s'interroger sur la possibilité d'utiliser une partie du bénéfice commercial que certains acteurs d'Internet en tirent pour mieux assurer la neutralité des réseaux.

Le rapport propose un consensus au-delà des partis. Il représente un travail de longue haleine sur un sujet où les choses vont vite.

Mme Françoise de Panafieu. Je voudrais revenir sur le sujet préoccupant que constitue la situation que l'on observe en Europe. J'insiste à nouveau sur le fait que le présent rapport, qui est véritablement formidable, devrait être traduit et adressé aux autres pays européens, de sorte que puisse être engagé ce travail commun dont vous déplorez précisément l'absence.

M. Patrick Bloche, rapporteur. Notre déplacement à Bruxelles, au cours duquel nous avons été reçus par le cabinet de Mme Neelie Kroes, nous a en effet déçus. Nous nous attendions à ce que les autorités européennes expriment une volonté plus claire, non pas de « corseter » ou de filtrer Internet, mais de mieux garantir les droits fondamentaux.

C'est pourquoi la résolution commune avec le *Bundestag* présente une grande importance. La proximité de nos approches laisse espérer que l'Allemagne et la France pourront, ensemble, faire bouger les choses sur les problèmes du numérique.

M. Patrice Verchère, rapporteur. Nos propositions sont également attendues à Washington comme nous l'ont indiqué nos interlocuteurs lors de notre déplacement aux États-Unis. Il est certain qu'elles auront plus de poids si l'Europe s'unit pour les soutenir.

M. Dominique Le Mèner. Je souhaite me faire l'écho d'une préoccupation identique à celle évoquée par Françoise de Panafieu. Il conviendrait de mettre en ligne une version anglaise du présent rapport, qui serait ainsi accessible à nos partenaires européens. Cela permettrait de les sensibiliser à ces sujets : cette tâche nous incombe également, compte tenu de l'importance des effets de la révolution numérique pour l'avenir.

M. Pierre Morel-A-L'Huissier. Vous avez fait part de l'audition par la mission du professeur de droit, M. Jean-Emmanuel Ray, qui connaît bien la question du télétravail. J'ai, pour ma part, présenté en 2006 un rapport sur le développement du télétravail. Il existe en France une certaine réticence sur ce sujet, par rapport aux comportements que l'on observe dans les pays anglo-saxons : aux États-Unis, quelque 28 % de la population active a recours au télétravail, quand ce taux est de l'ordre de 11 à 12 % en France. Par-delà les conclusions résultant de l'audition précitée, que faire pour favoriser l'évolution du télétravail en France ?

M. Philippe Gosselin. On ne peut occulter les difficultés qui existent pour harmoniser les situations qui prévalent respectivement en France et aux États-Unis. Les approches y sont très différentes pour ce qui concerne tant la notion de données personnelles - celle-ci inclut, aux États-Unis, les données de nature commerciale, qui sont l'objet d'échanges – que celle de libre circulation de l'information. En outre, les travaux menés depuis plusieurs années au plan européen par le groupe de travail sur la protection des données – le G 29 – attestent l'existence de difficultés pour s'accorder sur ces questions.

Une véritable ambition est évidemment nécessaire. Un travail doit être mené, sans doute avec l'Allemagne et d'autres partenaires. Mais une réelle détermination est de rigueur, car les obstacles sont nombreux.

M. Gilbert Mathon. Par-delà la question de la fracture numérique concernant les réseaux à haut débit – en cours de résorption –, il est essentiel de

mentionner celle qui concerne les réseaux à très haut débit, en particulier compte tenu de son impact sur la question du télétravail. Pour réduire cette fracture, plusieurs dizaines de milliards d'euros sont nécessaires et c'est pourquoi la mise en œuvre d'un plan national en faveur du développement du très haut débit est indispensable.

Or l'orientation n° 44 du présent rapport, relative à la réduction de la fracture numérique territoriale, n'aborde que partiellement ce thème. Une étude sur la généralisation du très haut débit serait nécessaire car la fracture numérique qui serait la conséquence de cette absence de généralisation aurait un impact sur notre économie et nos territoires extrêmement négatif.

M. le président Jean-Luc Warsmann. Je partage cette préoccupation. Il est vrai que des schémas régionaux sont en cours d'élaboration, ou que certains départements travaillent, à l'élaboration de schémas directeurs d'aménagement numérique (SDAN), de manière à réduire cette fracture.

Il faut rappeler qu'en moyenne, 70 % des coûts de déploiement de la fibre optique relèvent du génie civil. Or de nombreux travaux de voiries sont aujourd'hui conduits dans nos communes sans que soit suffisamment prise en compte la nécessité de prévoir des gaines pour ce déploiement, ce qui génère des situations de gâchis.

Il est indispensable, en vue de l'établissement d'un schéma général, de chiffrer le coût du déploiement de la fibre optique au profit de tous, tout en optimisant ces coûts par l'utilisation des gaines déjà existantes, sans quoi nous ne pourrons atteindre notre objectif d'accès de l'ensemble des territoires à la fibre optique et provoquerons le décrochage d'une partie d'entre eux.

Ces efforts doivent être engagés, que les opérateurs privés aient l'intention d'investir – conformément aux cartes de déploiement du très haut débit publiées récemment par le ministre chargé de l'aménagement du territoire – ou non.

Il convient par ailleurs de garder à l'esprit la question de l'accès des citoyens à la technologie de l'ADSL – service de base, si l'on peut dire –, qui n'est toujours pas assuré dans certaines zones.

M. Patrick Bloche, rapporteur. Notre rapport a d'abord porté sur les droits des individus. On a donc été conduit à réaffirmer le droit d'accès à Internet tant du point de vue social que territorial.

Il est vrai que nous avons été moins déçus par notre déplacement à Washington que par celui que nous avons fait à Bruxelles. Si, aux États-Unis, la conception des données personnelles peut paraître très différente de la nôtre en ce que les Américains les identifient volontiers avec des données commerciales dont le consommateur peut lui-même tirer bénéfice, il y existe néanmoins des mouvements représentant les consommateurs et la société civile extrêmement vigilants et qui interpellent fréquemment le Sénat et la Chambre des représentants.

L'entretien que nous avons eu avec un conseiller du Président Barack Obama nous a convaincus que la question des données personnelles n'était pas une question secondaire aux États-Unis. Il serait donc opportun de traduire en anglais nos 54 orientations ; une association américaine comme l'EPIC (*Electronic Privacy Information Center*) sera certainement très intéressée d'en prendre connaissance. Mais la première étape reste de convaincre nos partenaires européens si nous voulons que nos préconisations aient une portée plus large.

M. le président Jean-Luc Warsmann. Je vous remercie pour ce débat extrêmement intéressant.

La Commission, conjointement avec la commission des Affaires culturelles, autorise le dépôt du rapport de la mission d'information commune en vue de sa publication.

SYNTHÈSE DES ORIENTATIONS

TITRE PREMIER
L'INTERNET AU SERVICE DES DROITS DE L'INDIVIDU

PREMIÈRE PARTIE : LA LIBERTÉ D'EXPRESSION ET DE COMMUNICATION, L'ACCÈS À L'INFORMATION, LA CONNAISSANCE ET LA CULTURE À L'ÈRE NUMÉRIQUE

Orientation n° 1 : aider la presse d'information à se développer sur les nouveaux supports numériques

– clarifier et mieux cibler les aides attribuées dans le cadre du fonds d'aide au développement des services de presse en ligne (fonds SPEL) ;

– obtenir au plus vite l'autorisation d'appliquer un taux super-réduit de TVA à la presse en ligne ;

– dans le cadre de la réflexion sur une réforme globale des modalités d'intervention de l'État en faveur de la presse, s'assurer qu'un accent particulier soit porté sur le soutien à des stratégies d'investissement dans le développement numérique ;

– encourager les éditeurs de presse à développer *de façon concertée* des projets numériques permettant une meilleure valorisation de leurs contenus diffusés sur l'Internet et sur les plateformes mobiles ;

– s'assurer que *Google* respecte son engagement de permettre aux éditeurs de presse d'être exclus de *« Google Actualités* » sans pour autant être déréférencés du moteur de recherche ;

– charger l'Autorité de la concurrence d'examiner les pratiques d'*Apple* relatives à la vente d'abonnements à des titres de presse sur ses tablettes numériques (*Ipad*).

Orientation n° 2 : garantir une présence forte du service public audiovisuel sur les nouveaux supports numériques

Au-delà du discours sur la priorité que constituerait le « média global » et de la nomination d'un responsable identifié, M. Bruno Patino, sur ce sujet**,** il est impératif que le nouveau contrat d'objectifs et de moyens du groupe France Télévisions, en cours de négociation, prévoie une stratégie crédible et ambitieuse de développement numérique accompagnée d'un financement qui soient à la hauteur des enjeux.

Il convient par ailleurs de s'assurer de la gratuité de l'accès aux contenus du service public sur ces nouveaux supports.

Enfin, la mission souhaite que soit engagée une politique volontariste de mise à disposition de certains programmes libres de droits dans des conditions permettant leur (ré)utilisation libre et gratuite, dans une démarche de co-création avec les internautes.

Orientation n° 3 : établir un cadre favorable à la numérisation du patrimoine, vecteur exceptionnel de démocratisation de l'accès à la culture

La mission estime que la numérisation du patrimoine doit être considérée par les États comme une priorité pour l'avenir. Elle préconise par conséquent :

– que notre pays poursuive les efforts financiers en faveur de la numérisation du patrimoine ;

– que la France, qui a pris une longueur d'avance sur ses partenaires européens en la matière, incite ses partenaires européens à amplifier leurs efforts et à se doter d'un cadre commun définissant les modalités d'un partenariat équilibré avec les partenaires privés, tels que *Google*, pour faire respecter le droit d'auteur et éviter que ces derniers ne soient en position de dicter leurs conditions ;

– que l'on veille à ne pas « numériser pour numériser » mais que l'accent soit mis sur les moyens de faciliter et de développer l'accès par le plus grand nombre aux fonds numérisés, quels qu'ils soient (fonds de l'INA, de la BNF…), ce qui implique de réfléchir très en amont sur les moyens à mettre en œuvre pour qu'ils puissent être plus « repérables » (référencement, indexation des contenus, citations dans les blogs, les réseaux sociaux ou les sites les plus consultés, etc.) :

– que soit rapidement publié le décret qui doit préciser les dispositions du code du patrimoine, adoptées en 2006, dans le cadre de la loi n° 2006-961 relative aux droits d'auteur et aux droits voisins dans la société de l'information, par lesquelles la BNF, et accessoirement l'Institut national de l'audiovisuel (INA), se sont vus confier la mission du dépôt légal des documents créés sur support numérique.

Orientation n° 4 : assurer la sauvegarde des données numérisées

– débloquer les études sur le sujet. Engager rapidement une étude réellement scientifique des phénomènes de vieillissement des supports, notamment des supports optiques, visant à dégager des recommandations fiables en matière de standardisation de formats de supports d'archivage longue durée. Lancer rapidement un appel à projets ambitieux visant à remplacer la technologie d'enregistrement optique actuelle (CDR et DVDR), basée pour le moment sur des processus physico-chimiques complexes et mal contrôlés, par des technologies plus robustes et prévisibles ;

– **éviter la perte des compétences dans le privé et le public.** Prendre les mesures urgentes nécessaires à la préservation des compétences clés, avant qu'elles n'aient complètement disparu de l'Europe ;

– **favoriser l'innovation et l'apparition d'une offre industrielle de qualité.** Soutenir vigoureusement les quelques entreprises qui ont déjà effectué des avancées vers la réalisation de disques optiques numériques enregistrables de très bonne longévité ;

– **élaborer une véritable politique d'archivage numérique.** S'assurer au sein de chaque ministère que les données numériques importantes sont bien l'objet du suivi indispensable à leur survie. Évaluer l'intérêt d'une mutualisation des moyens, dans la perspective d'une stratégie active à l'échelon national, ou de la création d'un centre de conservation des données numériques à long terme équipé de robots permettant le suivi nécessaire à grande échelle.

Orientation n° 5 : garantir une répartition équitable de la valeur entre les grands moteurs de recherche et les agrégateurs de contenus d'une part et les médias traditionnels et producteurs de contenus d'autre part

Si un mécanisme permettant de taxer les recettes publicitaires des grands moteurs de recherche, type taxe « *Google* », venait à entrer en vigueur, il serait souhaitable d'inciter nos partenaires européens à instituer un même mécanisme de taxation, afin de ne pas pénaliser les annonceurs français et d'accroître l'efficacité de cette mesure.

Pour éviter que la télévision connectée ne fragilise trop les chaînes de télévision qui font l'objet d'une régulation importante et participent largement au financement de la création, il convient de conduire rapidement une réflexion sur les moyens d'assurer un équilibre entre acteurs traditionnels du secteur et nouveaux acteurs, tant en termes d'accès à la ressource publicitaire que de participation au financement de la création.

La mise en place d'obligations de financement de la production par les portails web nécessiterait en raison de leur caractère international une action concertée au plan mondial, ou au moins européen.

DEUXIÈME PARTIE : INTERNET, UN NOUVEL INSTRUMENT AU SERVICE DE LA DÉMOCRATIE

Orientation n° 6 : obtenir un engagement solennel de l'ONU reconnaissant la valeur d'Internet pour la promotion des droits de l'homme

Engager une action diplomatique visant à l'adoption par l'ONU d'une déclaration sur la liberté de communication par voie électronique au regard de l'importance acquise par ces techniques pour la défense et la promotion des droits de l'homme.

Orientation n° 7 : développer les sites Web des communes

Engager les services des administrations centrales compétentes à mieux informer les maires sur les conditions dans lesquelles ceux-ci peuvent créer, gérer et faire évoluer les sites Web communaux de sorte que tous les citoyens, en tout lieu du territoire national, puissent disposer, à égalité, des nouveaux outils numériques de démocratie locale.

Orientation n° 8 : renforcer l'expression démocratique sur les sites Web des collectivités territoriales

Rappeler par circulaire aux maires et présidents des organes délibérants des collectivités territoriales leur obligation de réserver un espace d'expression aux élus de l'opposition sur les sites Web présentant les actions de ces collectivités.

Orientation n° 9 : rendre plus transparentes les procédures d'organisation des débats publics sur Internet

Garantir à chaque citoyen participant à un débat public par le biais d'Internet la transparence des règles selon lesquelles sa participation est prise en compte. À cette fin, formuler des recommandations sur l'organisation de ces débats, leurs méthodes, leurs audits, la formation des organisateurs, lesquelles pourraient servir de référentiel pour les initiatives de e-démocratie prises par les institutions publiques. Cette mission pourrait revenir à la Commission nationale du débat public dans le cadre des compétences qui lui sont déjà reconnues.

Orientation n° 10 : mieux mesurer les risques de détournement que présentent les procédures de vote par Internet

Engager une évaluation indépendante et transparente des procédures de vote par le biais d'Internet.

TROISIÈME PARTIE : INTERNET, DE NOUVEAUX RAPPORTS ENTRE LES CITOYENS ET L'ÉTAT

Orientation n° 11 : maintenir un accès multicanal à l'administration

Garantir aux administrés que les procédures et les informations administratives dématérialisées demeurent accessibles par voie non numérique.

Orientation n° 12 : évaluer les procédures destinées à assurer la pérennité des documents administratifs dématérialisés

Dresser un bilan des actions entreprises et des questions tant techniques que juridiques que pose la conservation à long terme des documents administratifs dématérialisés.

Orientation n° 13 : améliorer l'accès aux données publiques et en permettre la réutilisation tout en garantissant la protection des données personnelles

– Rendre plus effectif le droit d'accès aux données publiques en précisant les dispositions légales en vigueur (article 17 de la loi du 17 juillet 1978) afin que tous les

organismes publics concernés recensent et rendent disponible en ligne l'ensemble de leurs données publiques communicables ;

– n'imposer une redevance pour la réutilisation des données que dans des cas exceptionnels ;

– obliger les administrations à recourir à des formats de fichiers qui permettent une exploitation documentaire des données qui y sont contenues ;

– garantir que l'ouverture des données publiques ne mettra pas en cause le principe de la protection des données personnelles.

Orientation n° 14 : évaluer les limites à poser à la réutilisation des données d'archives contenant des données personnelles

Clarifier le régime juridique de la réutilisation à des fins commerciales des archives contenant des données personnelles.

*
* *

TITRE DEUXIÈME
LE DROIT À UNE PROTECTION DANS L'UNIVERS NUMÉRIQUE

PREMIÈRE PARTIE : LE DROIT À LA VIE PRIVÉE : UNE PROTECTION À RÉINVENTER À L'ÈRE DU NUMÉRIQUE

Orientation n° 15 : protéger l'intimité des internautes en limitant les « recherches d'amis » sur les réseaux sociaux

Sur le modèle de l'exemple allemand, contraindre les réseaux sociaux à limiter les « recherches d'amis » à partir du carnet d'adresses mèl. de leurs utilisateurs, en offrant aux personnes concernées la possibilité de s'opposer à une utilisation de leur adresse mèl.

Orientation n° 16 : pour des systèmes de géolocalisation autorisés et non plus simplement déclarés auprès de la CNIL

Modifier l'article 25 de la loi du 6 janvier 1978, de manière à soumettre la mise en œuvre des traitements de géolocalisation à un régime d'autorisation par la CNIL et non de simple déclaration comme cela est actuellement le cas.

Orientation n° 17 : intégrer dans l'usage des puces *RFID* le respect de la vie privée

Renforcer la protection de la vie privée dans le cadre de l'utilisation des puces *RFID* :

— en interdisant à des tiers non autorisés l'accès aux informations qu'elles contiennent ;

— en rendant visibles leur présence par un son, une lumière ou un signal lorsqu'elles sont activées.

Orientation n° 18 : clarifier le statut juridique de l'adresse IP pour renforcer la protection des données personnelles qui lui sont liées

Orientation n° 19 : pour une destruction et une anonymisation complètes des données par les fournisseurs de services après six mois

Contraindre les fournisseurs de services, conformément aux recommandations du G29, d'une part, à détruire, après six mois de conservation, les références aux adresses IP des utilisateurs de ses services et, d'autre part, à anonymiser complètement ces données, jusqu'au dernier octet, pour rendre impossible toute reconstitution de l'adresse par rétro-ingénierie.

Orientation n° 20 : permettre à l'internaute, mieux informé, de contrôler ses données personnelles

Plutôt que de consacrer un droit général et absolu à l'oubli numérique, qui ne serait pas opérationnel, améliorer en amont l'information de l'internaute, en lui offrant des outils lui permettant d'assurer un meilleur contrôle de ses données personnelles.

Orientation n° 21 : instaurer un droit à l'oubli sur les réseaux sociaux

Prévoir, pour les seuls réseaux sociaux et non l'ensemble des sites Web, un droit à l'oubli dédié et adapté, reposant sur :

— un droit exprès et effectif à l'effacement de ses données et non un simple droit à la désactivation de son profil ;

— la garantie d'une procédure simple et facilement accessible, permettant d'effacer l'intégralité de ses données ou de les récupérer en vue de les réutiliser ;

— l'effacement par principe des données d'un profil d'utilisateur après un certain délai si aucun usage n'en est fait, l'utilisateur pouvant opter pour le non-effacement de ses données.

Orientation n° 22 : renforcer l'information des internautes en matière de ciblage publicitaire

Obliger les responsables de traitement collectant des données à caractère personnel par le biais de « *cookies* », notamment à des fins de ciblage publicitaire, d'informer l'internaute dans sa langue d'origine :

— des finalités et l'utilisation qui est faite de ses données de navigation ;

— de la nature des données personnelles ainsi collectées ;

— des personnes ou catégories de personnes habilitées à avoir accès à ces informations ;

— des moyens dont l'utilisateur dispose pour exprimer ou refuser son consentement ;

— des coordonnées d'un point de contact lui permettant ultérieurement d'exercer ses droits d'accès, de rectification et d'opposition.

Orientation n° 23 : développer des navigateurs Internet plus protecteurs et plus transparents en matière de ciblage publicitaire

Obliger les responsables de traitement collectant des données à caractère personnel par le biais de « *cookies* », notamment à des fins de ciblage publicitaire, d'informer l'internaute des possibilités de paramétrage dont l'utilisateur dispose depuis son navigateur Internet pour exprimer ou refuser son consentement. Il est cependant impératif que, dans le même temps, les navigateurs Internet offrent un réglage par défaut :

— protecteur des données personnelles au moment de l'installation ou de la mise à jour du navigateur ;

— transparent et facile à modifier ;

— fin, lui permettant de gérer ses préférences en fonction des caractéristiques des *cookies* et, à ce titre, de dire « *oui* », « *non* » ou « *je préfère* ».

Orientation n° 24 : assurer et préserver un haut niveau de protection des données en Europe

Dans le cadre de la révision de la directive du 24 octobre 1995, garantir un niveau de protection élevé et équivalent des données personnelles dans l'ensemble de l'Union européenne, en instaurant une nouvelle législation communautaire, le cas échéant, par voie de règlement.

Orientation n° 25 : obliger tout responsable de traitements à notifier les failles de sécurité

Dans le cadre de la révision de la directive du 24 octobre 1995, consacrer l'obligation pour tout responsable de traitements de données à caractère personnel de

notifier les failles de sécurité auprès de l'autorité nationale de protection des données personnelles – en France, la CNIL – et des particuliers concernés par ces violations.

Orientation n° 26 : renforcer l'information des personnes dont les données personnelles sont collectées

Dans le cadre de la révision de la directive du 24 octobre 1995, renforcer les obligations d'information incombant à tout responsable collectant des données personnelles, qui devront désormais informer de manière spécifique, claire et accessible la personne concernée :

— des coordonnées du responsable du traitement et, le cas échéant, de celle de son représentant ;

— de la durée de conservation des données collectées et des critères qui la justifient ;

— des coordonnées du service auprès duquel les droits d'accès, de rectification et de suppression peuvent s'exercer.

Ces informations et, plus largement, les conditions d'utilisation ainsi que les rubriques « *Vie privée* » devront impérativement être traduites dans la langue d'origine de l'utilisateur.

Orientation n° 27 : exclure du *cloud computing* réalisé hors de l'Union européenne les données personnelles dites « sensibles »

Dans le cadre de la révision de la directive du 24 octobre 1995, exclure du *cloud computing* réalisé hors de l'Union européenne le traitement de données personnelles sensibles ou comportant certains risques pour les personnes concernées, comme les données biométriques, les données génétiques, les données judiciaires, les données financières ou les données concernant des enfants.

Orientation n° 28 : soumettre les acteurs du *cloud computing* à des audits de sécurité réguliers

Dans le cadre de la révision de la directive du 24 octobre 1995, faire obligation aux acteurs du *cloud computing* de réaliser régulièrement des audits de sécurité.

Orientation n° 29 : renforcer l'indépendance du groupe de travail G29

Dans le cadre de la révision de la directive du 24 octobre 1995, renforcer l'indépendance du groupe de travail G29, en le dotant de moyens humains et financiers propres.

Orientation n° 30 : faire du « *privacy by design* » un atout majeur pour l'Europe

Encourager et renforcer au sein de l'Union européenne la recherche, l'innovation et le développement dans le secteur des technologies respectueuses de la vie privée dès leur conception, dites « *privacy by design* », afin de doter l'Europe d'une véritable politique industrielle du numérique et lui permettre ainsi de bénéficier d'un indéniable avantage comparatif dans la compétition mondiale.

Orientation n° 31 : mettre fin aux difficultés liées à l'extraterritorialité du droit applicable en matière de protection des données

Dans le cadre de la révision de la directive du 24 octobre 1995, assurer le même niveau de protection de la vie privée et des données personnelles à tous les résidents de l'Union européenne, indépendamment du lieu d'établissement du responsable du traitement.

Soumettre, pour ce faire, tous les responsables de traitement, où qu'ils se trouvent et même s'ils sont établis hors de l'Union européenne, aux juridictions et au droit des États membres dès lors qu'ils visent les publics qui y résident.

Orientation n° 32 : une action diplomatique forte pour l'adoption d'une convention internationale en matière de protection de la vie privée

À court terme, adopter au Parlement français, en application de l'article 34-1 de la Constitution, une résolution visant à soutenir la signature d'une convention internationale sur la protection de la vie privée et des données personnelles.

À moyen terme, promouvoir par l'action diplomatique conjointe de la France et de l'Union européenne l'adoption d'une convention internationale sous l'égide de l'ONU relative à la protection de la vie privée et des données personnelles.

DEUXIÈME PARTIE : LA SÉCURITÉ DES ÉCHANGES DE DONNÉES SUR LES RÉSEAUX : UNE GARANTIE NÉCESSAIRE

Orientation n° 33 : renforcer les procédures d'information en cas de faille de sécurité

Mettre en place un dispositif d'information de l'Agence nationale de la sécurité des systèmes d'information en cas de faille de sécurité importante sur un réseau informatique.

Orientation n° 34 : mieux évaluer l'importance et les conséquences des transferts de données personnelles dans le cadre du *cloud computing*

Établir un bilan d'évaluation des transferts de données personnelles effectués dans le cadre de l'externalisation des traitements informatiques en dehors de l'Union

européenne. Ce bilan aurait pour but de mieux appréhender l'ampleur de ce phénomène, en particulier celui des sous-traitances en cascades, et d'évaluer l'effectivité des différents dispositifs légaux en jeu au regard de la nécessité de préserver les droits des personnes concernées.

TROISIÈME PARTIE : LES DROITS DES MINEURS DANS L'UNIVERS NUMÉRIQUE

Orientation n° 35 : Promouvoir le droit à la déconnexion

Le droit pour les salariés de ne pas être connecté constamment à leur outil de travail numérique doit être promu au sein des entreprises.

Orientation n° 36 : renforcer l'éducation aux médias et la place du numérique à l'école :

– mettre en place un enseignement spécifique d'éducation au numérique dans le cadre de l'éducation civique, conformément aux dispositions de la loi n° 2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques et réfléchir à son articulation avec le B2i ;

– dans le cadre du B2i, donner plus d'importance à l'apprentissage de l'usage responsable de l'Internet. Développer davantage le B2i à l'école primaire ;

– améliorer la formation des enseignants aux outils et services numériques ;

– permettre à chaque élève de disposer d'un outil individuel et mobile permettant de se connecter au réseau de l'école ou de l'établissement ;

– généraliser les espaces numériques de travail (ENT) ;

– créer de nouveaux supports interactifs et des manuels numériques innovants ;

- lancer une réflexion sur une réforme plus globale des programmes et des méthodes d'enseignement et d'évaluation afin de mettre le numérique au service d'une pédagogie renouvelée.

Orientation n° 37 : renforcer le contrôle parental

Organiser une grande campagne d'information et de sensibilisation sur les technologies du numérique et le bon usage par les mineurs de ces dernières, basée sur le slogan « 3, 6, 9, 12 » : pas de télévision avant 3 ans ; pas de console de jeux personnelle avant 6 ans ; l'accès à Internet, accompagné d'un adulte, à partir de 9 ans ; et enfin un usage individuel d'Internet à partir de 12 ans.

Par ailleurs un véritable travail d'information doit être effectué, sur trois points :

– ce que l'on publie sur Internet y demeure éternellement ;

– ce que l'on y met peut tomber dans le domaine public ;

– ce que l'on y trouve ne doit pas être pris pour argent comptant.

Améliorer l'utilisation et la qualité des logiciels de contrôle parental.

Orientation n° 38 : renforcer la mission d'éducation aux médias de l'audiovisuel public

Les études ayant montré que plus il existe une offre de programmes adaptés aux enfants, en télévision ou en ligne, moins ces derniers sont enclins à aller vers des contenus à risques, la mission préconise de faire de France 4 la chaîne jeunesse du groupe France Télévisions. Cette chaîne ne comporterait pas de publicité et proposerait notamment des programmes et des campagnes d'information permettant de sensibiliser les enfants, les adolescents et les jeunes adultes aux opportunités et aux risques liés au numérique.

Orientation n° 39 : renforcer le rôle des médias dans l'éducation au numérique

– obliger les chaînes de télévision et de radio privées de définir un engagement annuel d'actions sur ce thème sous le contrôle du CSA ;

– encourager les jeunes à être créateurs de médias en mettant à leur disposition sur Internet des espaces publics dans lesquels ils pourraient publier leurs créations personnelles.

Orientation n° 40 : confier au Conseil national du numérique un rôle ambitieux de corégulation en matière de prévention et d'éducation aux médias

La mission estime qu'il incomberait à un Conseil national numérique reconfiguré selon les préconisations formulées dans la dernière partie du présent rapport de se saisir de la question prioritaire de la prévention et de l'éducation aux médias en réunissant les institutions publiques, les associations, les chercheurs, les professionnels des médias et des réseaux (télévisions et radios publiques comme privées, fournisseurs d'accès à Internet, sites et portails Internet...)

Au-delà de la mission d'élaboration et de suivi des chartes de bonne conduite, la mission du Conseil serait multiple :

– assurer une veille sur les actions d'éducation aux médias et constituer un Observatoire des usages des technologies numériques par les mineurs ;

– créer un portail consacré à l'éducation aux médias, rassemblant les ressources utilisées sur tous les supports ; faire émerger des ressources validées d'éducation aux médias, disponibles pour le plus grand nombre ; soutenir des actions, d'information, de communication, notamment des différents médias, des collectivités, des associations ;

– contrôler l'élaboration de systèmes de contrôle parental simples et de qualité et assurer un suivi de l'utilisation qui en est faite par les parents ;

– être un lieu de dialogue entre l'ensemble des acteurs.

S'agissant de la charte sur la publicité ciblée, la mission souhaite que l'interdiction du ciblage, qui concerne actuellement les moins de treize ans, soit élargie aux moins de seize ans.

Orientation n° 41 : renforcer la corégulation au plan européen en mettant l'accent sur plusieurs priorités :

– agir de façon concertée pour contraindre les réseaux sociaux à appliquer plus strictement l'interdiction de s'inscrire avant un certain âge. La mission déplore que l'entreprise *Facebook* mette aussi peu de diligence et de responsabilité à protéger les enfants qu'elle en a mis à répondre aux questions de notre mission sur l'ensemble de ces sujets. Or, malgré la difficulté technique de procéder à un contrôle systématique et préalable de l'âge des utilisateurs, il lui est loisible de renforcer l'information sur cette interdiction et de procéder à des contrôles réguliers ainsi qu'à des annulations de comptes lorsqu'il s'avère qu'un membre a de toute évidence moins de 13 ans ;

– obtenir des engagements clairs des opérateurs, des hébergeurs et des éditeurs de site (sur le modèle de la Charte des sites communautaires signée au niveau européen) sur l'information qu'ils sont prêts à mettre en place, en ce qui concerne la protection des mineurs et plus généralement leur responsabilité sociale vis-à-vis des jeunes. Ces messages d'information ne devraient pas seulement être bien exposés sur les sites Internet, à des emplacements visibles et accessibles, ils devraient également être envoyés aux internautes lors de l'ouverture d'une adresse de courriel par tous les FAI (fournisseur d'accès à Internet) et les hébergeurs de boîtes de courriels, accompagner tout logiciel de contrôle parental et s'afficher lors de l'ouverture d'un blog ou d'un compte sur un réseau social. M. Thomas Jarzombek, député allemand, président, au sein de la commission d'enquête mise en place par le *Bundestag*, des groupes de travail sur la protection des mineurs et l'éducation aux médias, a souligné, s'agissant de la protection des mineurs sur les réseaux sociaux, l'efficacité des campagnes d'information à l'aide de la « communication virale » [(1)]. Il a indiqué que de telles campagnes avaient permis de lancer avec succès des messages d'avertissement en direction des jeunes filles qui mettent sur Internet des photos d'elles-mêmes en petite tenue. Plus de la moitié des utilisateurs aurait modifié son comportement suite à cette initiative. Il conviendrait par conséquent d'inciter les grands acteurs d'Internet à se mettre d'accord pour lancer ce type de campagnes d'information ;

– l'effort d'information pourrait aussi concerner le signalement des contenus choquants ou incitant à des comportements à risque. Aujourd'hui, les pages de signalement des contenus choquants ne sont pas toujours facilement accessibles et sont parfois assez complexes, avec des formulaires à remplir. Ces pages pourraient être accompagnées d'une vidéo de démonstration pour que leur usage soit facilité.

*

* *

(1) Les messages sont transmis de proche en proche par les utilisateurs. Cette technique est utilisée par le marketing et passe essentiellement par les réseaux sociaux.

TITRE TROISIÈME
LE DROIT À L'ACCÈS À INTERNET

PREMIÈRE PARTIE : QUELLE NEUTRALITÉ DE L'INTERNET ?

Orientation n° 42 : Une évaluation des mesures de blocage légal

Notre mission estime :

– que l'ensemble des éléments qui a été porté à sa connaissance justifie *a minima* qu'il soit procédé à une évaluation des mesures de blocage légal – aucun nouveau cas de filtrage n'étant ajouté aux cas existants en attendant ;

– et que l'intervention du juge doit être prévue dans tous les cas de blocage légal.

Orientation n° 43 : élargir la notion de neutralité de l'Internet aux autres acteurs du Web

La mission estime qu'une réflexion approfondie est nécessaire sur la neutralité des moteurs de recherche. Le caractère mondial des principaux moteurs de recherche implique que cette réflexion soit menée au plan européen voire international.

Par ailleurs, une réflexion prospective approfondie sur les télévisions connectées doit être lancée afin que soit maintenue l'ouverture des terminaux et des principales plateformes de services.

DEUXIÈME PARTIE : AMÉLIORER L'ÉGALITÉ DANS LES CONDITIONS D'ACCÈS À INTERNET : LA LUTTE CONTRE LES FRACTURES NUMÉRIQUES

Orientation n° 44 : réduire la fracture numérique territoriale

– La mission souhaite que des mécanismes de soutien soient mis en œuvre par exemple sous forme de dispositifs de péréquation en faveur des territoires menacés par la fracture numérique territoriale ;

– la mission souhaite aussi que soit exploré l'ensemble des opportunités offertes par toutes les technologies disponibles afin d'améliorer la desserte des territoires, en attendant le déploiement effectif de la fibre.

Orientation n° 45 : permettre un accès au haut débit à bas coût pour les plus démunis

La mission souhaite la mise en place d'une véritable tarification sociale de l'Internet, ce qui suppose néanmoins une modification de la directive 2009/136/CE du 25 novembre 2009 afin que l'accès à Internet à haut débit devienne une composante du service universel des communications électroniques.

Orientation n° 46 : poursuivre le déploiement du réseau d'espaces numériques publics (EPN) et développer, en leur sein, l'accompagnement du public dans l'usage des technologies numériques

La mission estime qu'il s'agit d'un moyen efficace de réduire l'inégalité numérique dont sont victimes les personnes ne disposant pas d'ordinateur, d'accès au réseau ou de la connaissance technique nécessaire pour les utiliser.

Orientation n° 47 : développer le B2i adultes

Comme la Ligue de l'enseignement, la mission estime qu'« *en attendant que toute la population soit passée par les formations B2i École, Collège et Lycée, le B2i adultes est en effet une réponse au problème de la fracture numérique qui touche toutes les générations.* »

Orientation n° 48 : favoriser et développer les initiatives permettant de mettre des ordinateurs à disposition des personnes qui n'en disposent pas à travers

– la mise en place dans les logements sociaux d'ordinateurs connectés ;

– la mise à disposition des familles défavorisées des ordinateurs reconditionnés.

Orientation n°49 : garantir à l'internaute qu'il ne sera pas dépossédé de son ordinateur personnel dans le cadre d'une procédure de saisie

Ajouter à la liste des biens insaisissables, telle que l'a fixée le décret du 31 juillet 1992, la mention de l'ordinateur personnel afin que les personnes faisant l'objet d'une saisie mobilière ne se voient pas fermer l'accès au monde numérique.

Orientation n° 50 : aider les personnes en difficultés pour raisons financières à conserver leur accès à Internet

Orientation n° 51 : rendre Internet plus accessible aux personnes handicapées

– Organiser une campagne d'information en direction des créateurs de sites Internet pour les sensibiliser aux problèmes de l'accessibilité numérique pour les personnes handicapées ;

– rendre obligatoire dans la formation des ingénieurs en informatique un enseignement relatif à l'accessibilité numérique pour les personnes handicapées, à l'instar de ce qui existe pour la formation des architectes.

Orientation n° 52 : réduire le fossé générationnel

– installer des espaces numériques dans les maisons de retraite et les accueils de jour ;

– organiser un accompagnement des personnes âgées dans l'apprentissage d'Internet à domicile (utilisation de la messagerie électronique, aide au remplissage de formulaires électroniques…) par les jeunes en service civique.

*

* *

TITRE QUATRIÈME

QUELLE GOUVERNANCE AU SERVICE DE CES DROITS ?

Orientation n° 53 : assurer une plus grande coordination et renforcer le dialogue entre les différents régulateurs concernés par la régulation de l'Internet

La mission estime qu'un rapprochement et une plus grande coordination entre ces diverses entités sont indispensables. S'agissant par exemple d'un sujet comme la neutralité de l'Internet, il est évident qu'il ne saurait être l'affaire du seul régulateur sectoriel en charge des « tuyaux », c'est-à-dire l'ARCEP. Le régulateur ayant compétence sur les contenus, à savoir le CSA, mais également la CNIL et l'autorité de la concurrence ont également un rôle à jouer. De même, le développement des téléviseurs connectés devrait inévitablement amener les régulateurs à coordonner leurs efforts.

Orientation n° 54 : préconisations relatives au Conseil national du numérique

La mission déplore la disparition d'une structure de médiation et de régulation telle que le Forum des droits sur Internet. Elle appelle de ses vœux le retour à une composition plus représentative de l'ensemble des parties prenantes de l'univers numérique, notamment les représentants des ayants droit, des associations de consommateurs et plus largement de la société civile, et un modèle plus ambitieux d'enceinte de corégulation disposant de l'ensemble des compétences qui étaient celles du Forum des droits sur Internet, en particulier celle de médiation et d'élaboration et de suivi de chartes de bonnes conduites.

LISTE DES PERSONNES AUDITIONNÉES ET DES DÉPLACEMENTS EFFECTUÉS PAR LA MISSION

Mercredi 5 mai 2010

— M. Bernard BENHAMOU, délégué aux usages de l'Internet

- *École Polytechnique*

  — M. Thomas CLAUSEN, maître de conférences

  — M. Fabrice LE FESSANT, chargé d'enseignement

Mercredi 19 mai 2010

- *Conseil supérieur de l'audiovisuel (CSA)*

  — M. Michel BOYON, président

  — M. Emmanuel GABLA, conseiller

  — M. Olivier JAPIOT, directeur général

- *Commission nationale de l'informatique et des libertés (CNIL)*

  — M. Alex TÜRK, président

Mardi 25 mai 2010

Table ronde

- *Fédération internationale des ligues des droits de l'homme*

  — M. Jean-Sébastien MARIEZ, membre du groupe de travail « Liberté et technologies de l'information et de la communication »

- *Nouveaux Droits de l'homme*

  — M. Pierre BERCIS, président

- *Association Informatique et Libertés*

  — Mme Ariane ROORYCK, secrétaire

- *Association IRIS*

  — Mme Meryem MARZOUKI, présidente

Mercredi 2 juin 2010

- *Forum des droits sur Internet (FDI)*
  - — Mme Isabelle FALQUE-PIERROTIN, présidente

Mardi 8 juin 2010

- *Bouygues Télécom*
  - — M. Emmanuel FOREST, vice-président, directeur général délégué
  - — Madame Brigitte LAURENT, directrice de la communication externe et institutionnelle
- *Iliad-FREE*
  - — M. Maxime LOMBARDINI, directeur général
  - — M. Olivier de BAILLENX, directeur des relations institutionnelles
  - — M. Alexandre ARCHAMBAULT, directeur des affaires réglementaires
- *SFR*
  - — M. Frank ESSER, président-directeur général
  - — M. Philippe LOGAK, secrétaire général
  - — M. Arnaud LUCAUSSY, directeur de la réglementation et des études économiques

Mercredi 16 juin 2010

- *Commission nationale consultative des droits de l'homme*
  - — M. Jean-Michel QUILLARDET, membre
  - — Mme Judith KLEIN, chargée de mission
- *Numéricable-Completel*
  - — M. Pierre DANON, président-directeur général
  - — M. Jérôme YOMTOV, secrétaire général

Mardi 22 juin 2010

- *Association des fournisseurs d'accès et de services Internet (AFA)*

  — M. Richard LALANDE, président

- *Fédération française des Télécoms*

  — M. Yves LE MOUËL, directeur général

- *France Télécom/Orange*

  — M. Stéphane RICHARD, directeur général

  — Mme Christine ALBANEL, directrice de la communication

  — M. Pierre-Antoine BADOZ, directeur des affaires publiques

  — Mme Florence CHINAUD, directrice des relations institutionnelles

Mercredi 30 juin 2010

— M. Dominique WOLTON, directeur du laboratoire « Information, Communication et Enjeux scientifiques » au CNRS

- *Autorité de régulations des communications électroniques et des postes (ARCEP)*

  — M. Jean-Ludovic SILICANI, président

  — M. Philippe DISTLER, directeur général

  — M. Stéphane HOYNCK, directeur des affaires juridiques

Mardi 6 juillet 2010

- *Renaissance Numérique*

  — M. Guillaume BUFFET, co-président

  — M. Loïc BODIN, délégué général

  — M. Etienne DROUARD, avocat à la cour

  — M. Marc LOLIVIER, membre du conseil d'administration, délégué général de la Fédération du *e*-commerce et de la vente à distance

— M. Thibaut MUNIER, directeur général de la société *Mille mercis*

Mercredi 8 septembre 2010

- *Facebook*

  — M. Richard ALLAN, directeur Europe de la politique publique

- *Google France*

  — M. Yoram ELKAÏM, directeur juridique « *Southern and Eastern Europe, Middle East and Africa* »

  — M. Olivier ESPER, chargé des relations institutionnelles

  — Mme Alexandra LAFERRIÈRE, chargée des relations institutionnelles

Mardi 14 septembre 2010

- *Yahoo ! France*

  — Mme Brigitte CANTALOUBE, directrice générale

  — M. Justin WEISS, directeur de la politique internationale en matière de données personnelles

  — M. Chris SHERWOOD, directeur européen de la politique publique

- *Skyrock.com /Orbus SA*

  — M. Pierre BELLANGER, président-directeur général de la société Orbus SA, groupe de communication gérant le réseau FM *Skyrock* et *Skyrock.com*

  — M. Jérôme AGUESS, directeur de la production Web

  — M. Olivier LANGLESS, directeur juridique

Mercredi 29 septembre 2010

- *Microsoft France*
  - — M. Marc MOSSÉ, directeur des affaires publiques et juridiques
  - — M. Jean GONIÉ, responsable des affaires institutionnelles
- *Association des services Internet communautaires (ASIC)*
  - — M. Giuseppe de MARTINO, président
  - — M. Benoît TABAKA, secrétaire général

Mardi 5 octobre 2010

- *Groupement des éditeurs de contenus et de services en ligne (GESTE)*
  - — M. Étienne DROUARD, avocat, président de la commission juridique du Geste
  - — M. Maxime JAILLET, juriste
  - — M. Guillaume MONNET, juriste
- *Dailymotion*
  - — M. Martin ROGARD, directeur France

Mardi 19 octobre 2010

- *SNCF*
  - — M. Jean-Luc DUFOURNAUD, directeur juridique délégué, correspondant « informatique et libertés »
  - — M. Sylvain THIRY, responsable de la sécurité des systèmes d'information
  - — M. Eric RAVY**,** directeur juridique de *voyages-sncf.com*

- *RATP*

  — M. Thien THAN-TRONG, directeur du département des systèmes d'information et télécommunication

  — M. Dominique CHAUMET, correspondant « informatique et libertés »

- *Groupe Laser-Cofinoga*

  — M. Philippe LEMOINE, président

  — M. Jean-Yves GODARD, directeur des relations extérieures

Jeudi 21 octobre 2010

Déplacement à Bruxelles auprès des instances communautaires

- *Contrôleur européen de la protection des données (CEPD)*

  — M. Giovanni BUTTARELLI, contrôleur adjoint

  — M. Laurent BESLAY, coordinateur sécurité et technologie

  — Mme Anne-Christine LACOSTE, conseiller juridique

- *Commission européenne*

  — M. Luis ROMERO REQUENA, directeur général du service juridique

  — M. Paolo STANCANELLI, adjoint au directeur général

  — Mme Lorena BOIX-ALONSO, chef de cabinet adjoint de Mme Nellie Kroes, commissaire européen en charge de la stratégie numérique

  — M. Hervé DUPUIS, membre du cabinet de Mme Nellie Kroes

- *Représentation permanente de la France auprès de l'Union européenne*

  — M. Pierre-Antoine MOLINA, conseiller justice

  — M. Romain BONENFANT, conseiller télécoms

- *Direction générale de la société de l'information et des médias*

  — Mme Megan RICHARDS, directrice des affaires générales

  — Mme Anne BUCHER, directrice des ressources

  — M. Bernd LANGEHEINE, directeur de la politique des communications électroniques

Mercredi 27 octobre 2010

Table ronde autour de la *e*-réputation

  — M^e^ Alain BENSOUSSAN, avocat à la cour d'appel de Paris

  — M^e^ Olivier SCHNERB, avocat à la cour d'appel de Paris

Mercredi 3 novembre 2010

- *Union fédérale des consommateurs « Que choisir ? »*

  — M. Serge MOLINARI, administrateur

  — M. Édouard BARREIRO, chargé de mission « nouvelles technologies »

  — Mme Catalina CHATELIER, juriste

- *Institut national de la consommation (INC)*

  — Mme Patricia FOUCHER, juriste

- *Centre de liaison de l'enseignement et des médias d'information (CLEMI)*

  — Mme France RENUCCI, directrice

Mardi 9 novembre 2010

Table ronde

— M. Serge TISSERON, psychologue et psychiatre

- *Collectif interassociation Enfance et Médias*

— Mme Sophie JEHEL, membre du conseil scientifique

- *Association e-enfance*

— Mme Justine ATLAN, directrice

— Mme Dominique DELORME, responsable de la ligne « Net Ecoute »

- *Action innocence*

— Mme Véronique FIMA-FROMAGER, directrice

- *Internet sans crainte*

— Mme Deborah ELALOUF, présidente-directrice générale de la société Tralalere, société en charge de l'animation du programme « Internet sans crainte »

— Mme Émilie PEINCHAUD, chargée de communication

- *Innocence en danger*

— Mme Sandra BELLARIVA, responsable des relations publiques

— Mme Laurence BENEUX, bénévole

Mercredi 10 novembre 2010

— M^e^ Winston MAXWELL, avocat à la cour d'appel de Paris

Mardi 16 novembre 2010

— Mme Myriam QUEMENER, substitut du procureur général près la cour d'appel de Versailles, auteur de *Cybercriminalité : droit pénal appliqué*

- *Agence nationale de la sécurité des systèmes d'information (ANSSI)*

— M. Patrick PAILLOUX, directeur

Mercredi 1er décembre 2010

- *Institut national de l'audiovisuel (INA)*

— M. Mathieu GALLET, président-directeur général

- *Bibliothèque nationale de France (BNF)*

— M. Bruno RACINE, président

Mercredi 8 décembre 2010

Table ronde

- *Association des maires ruraux de France*

— M. Fabrice DALONGEVILLE, président des maires ruraux de l'Oise

- *Association des maires des grandes villes*

— M. Olivier DEVILLERS, chargé de mission « technologies de l'information et de la communication »

- *Association des maires de France*

— M. Marc-Antoine JAMET, maire de Val-de-Reuil

- *Commission nationale du débat public*

— M. Philippe MARZOLF, vice-président

— M. Jean-François BÉRAUD, secrétaire général

Mardi 14 décembre 2010

— Lieutenant-colonel Éric FREYSSINET, service technique de recherches judiciaires et de documentation (STRJD), chef de la division de lutte contre la cybercriminalité

- *Direction générale de la modernisation de l'État (DGME)*

  — M. Arnaud LACAZE, chef du service « projets »

  — M. Perica SUCEVIC, conseiller juridique

Mercredi 19 janvier 2011

- *Réunion commune des membres de la mission sur les droits de l'individu dans la révolution numérique à l'Assemblée nationale et des membres de la commission d'enquête du* Bundestag

  Parlementaires, membres de la commission d'enquête

  — M. Axel E. FISCHER, président (CDU/CSU)

  — M. Jens KOEPPEN (CDU/CSU)

  — M. Lars KLINGBEIL (SPD)

  — M. Manuel HÖFERLIN (FPD)

  — M. Thomas JARZOMBEK (CDU/CSU)

  — Dr. Reinhard BRANDL (CDU/CSU)

  — M. Jimmy SCHULTZ (FPD)

  — M. Konstantin von NOTZ (*Bündnis 90 / Die Grünen*)

  Expertes, membres de la commission d'enquête

  — Mme Constanze KURZ

  — Mme Cornelia TAUSCH

Mercredi 2 février 2011 - vendredi 4 février 2011

- **Déplacement des rapporteurs aux États-Unis**

Mercredi 2 février 2011

— M. Marc ROTENBERG, *Executive Director*, *Electronic Privacy Information Center (EPIC)*

— M. Alex HOEHN-SARIC, *Counsel*, bureau du sénateur Jay ROCKEFELLER, president du *Commerce, Science and Transportation Committee*

— Mme Shelley HUSBAND, *Chief of staff* du député Bob GOODLATTE.

Jeudi 3 février 2011

— M. Darrell WEST, *Vice President and Director of Governance Studies, founding director of the Center for Technology Innovation at Brookings Technology Innovation – The Brookings Institution*

— M. Aneesh CHOPRA, *Chief technology Officer*, Maison Blanche

— M. Ed FELTEN, *Chief Technologist, Federal Trade Commission (FTC)*

— Mme Mignon CLYBURN, *Commissioner, Federal Communications Commission (FCC)*

— Mme Nancy LIBIN, *Chief Privacy Officer, Department of Justice*

Vendredi 4 février 2011

— M. Robert D. ATKINSON, *President, Information Technology and Innovation Foundation (ITIF)*

Mercredi 16 février 2011

Table ronde

- *Fédération des aveugles et handicapés visuels de France*

  — M. Rui GONCALVES, directeur général

  — M. Christian LAINÉ, formateur informatique

- *Association Valentin Haüy*

  — M. Fernando PINTO da SILVA, responsable du centre d'évaluation et de recherche sur les technologies pour les aveugles et les malvoyants (CERTAM)

- *Association BrailleNet*

  — M. Dominique BURGER, président

Mercredi 2 mars 2011

— M. Jean-Emmanuel RAY, professeur de droit du travail à l'Université Paris I-Sorbonne

Mercredi 30 mars 2011

— Dr Joseph NAOURI, pédopsychiatre

Mercredi 13 avril 2011

— M. Daniel KAPLAN, délégué général de la Fondation pour l'Internet nouvelle génération

Jeudi 14 avril 2011

— M. Jean-Marc MANACH, journaliste

ANNEXES

ANNEXE N°1 : COMPTE RENDU DE LA RÉUNION PARLEMENTAIRE FRANCO-ALLEMANDE DU 19 JANVIER 2011

ASSEMBLÉE NATIONALE

Deutscher Bundestag

Enquete-Kommission Internet und digitale Gesellschaft

Mission d'information
sur les droits de l'individu dans la révolution numérique

Le 19 janvier 2011

Assemblée nationale – Bundestag

Réunion commune

(par visioconférence)

Mission d'information de l'Assemblée nationale
sur les droits de l'individu dans la révolution numérique
Commission d'enquête du *Bundestag*
sur Internet et la société numérique

La séance est ouverte à 16 heures 15

M. Jean-Luc Warsmann, président, ***(Assemblée nationale)*** **–** Monsieur le président Axel Fischer, chers collègues du *Bundestag*, je voudrais tout d'abord vous adresser mes salutations, au nom de la mission d'information française, et plus particulièrement saluer le président Fischer que je suis heureux de revoir après notre rencontre à Paris, l'automne dernier.

Je suis également très heureux que nous puissions organiser aujourd'hui cette première réunion commune franco-allemande autour de la question de la révolution numérique. Je ne crois pas qu'il y ait beaucoup de précédents – sans

doute, aucun – d'une telle réunion commune entre une mission de contrôle de l'Assemblée nationale et une commission d'enquête du *Bundestag*.

Sans nous concerter, nos deux assemblées ont décidé, presque en même temps, de mener des investigations sur la question des droits de l'individu dans la révolution numérique, au printemps dernier.

Cela montre, s'il en était besoin, que ce sujet préoccupe beaucoup nos concitoyens, allemands et français, mais plus largement européens. Je crois qu'il est essentiel que les assemblées parlementaires puissent ouvrir la voie à une initiative commune franco-allemande dans ce domaine.

La mission d'information de l'Assemblée nationale comporte 20 membres issus de la commission des Lois et de la commission des Affaires culturelles. Créée le 7 avril 2010, elle rendra ses conclusions au printemps. Notre rapport doit mettre à plat toutes les questions auxquelles nos sociétés sont confrontées sur ce sujet et sera une force de propositions très concrètes.

Notre commission est animée par deux rapporteurs : M. Patrice Verchère, député du Rhône, qui appartient à la majorité et M. Patrick Bloche, député de Paris, de l'opposition. Ils interviendront lors de nos débats avec nos autres collègues membres de la mission : M. Sébastien Huyghe, vice-président de la mission, député du Nord et M. Marcel Rogemont, député d'Ille-et-Vilaine, en Bretagne.

Nous avons tenu plus de quarante auditions en recevant des experts des questions numériques de tous les horizons, des techniciens, des juristes, des associations de consommateurs, de défense des droits de l'homme, des intellectuels. Nous avons également auditionné les représentants des grands groupes de fournisseurs d'accès, les représentants de *Google, Facebook, Yahoo !, Microsoft*. Nous avons entendu les autorités de régulation françaises.

Nous avons également envoyé des questionnaires précis à *Google, Yahoo !* et *Facebook* pour compléter des auditions qui, pour certaines d'entre elles, ont été décevantes. Nous attendons beaucoup de ces réponses sur le droit à l'oubli, le respect de la vie privée, la protection des mineurs. Pour l'instant nous n'avons pas été totalement convaincus par les grands groupes que nous avons entendus. Ils ont tenu un discours très policé, très lisse et semblent parfois avoir essayé d'éluder les questions compliquées.

Une délégation de la mission s'est également rendue à Bruxelles où nous avons rencontré des représentants de la Commission européenne et nos deux rapporteurs se rendront également aux États-Unis dans quelques jours.

Deux lignes directrices ont structuré à ce jour les travaux de la mission : d'une part, aborder la révolution numérique du point de vue de la protection des droits de l'individu, d'autre part, considérer cette révolution comme l'occasion de promouvoir certains droits, ces deux aspects étant liés.

La révolution numérique offre de formidables opportunités en matière d'éducation, de culture, de science, dans tous les domaines de la connaissance humaine.

Mais elle ne doit pas être obscurcie par les risques qui pourraient naître de pratiques que nous ne pouvons que réprouver.

La protection des données personnelles nous préoccupe beaucoup. Je pense à la biométrie, la géolocalisation, les puces électroniques *RFID* mais aussi aux réseaux sociaux, tels que *Facebook*, et les moteurs de recherche, tels que *Yahoo !* et *Google*.

L'exportation des données personnelles dans le cadre du « *cloud computing* » et la localisation des *data centers* est aussi un sujet qui nous semble devoir être examiné de près. Il y a derrière cela des enjeux d'indépendance nationale et européenne majeurs sur lesquels nous devrons, certainement, avoir des positions fortes.

Nous travaillons aussi sur l'intérêt de reconnaître ou pas un droit à l'oubli numérique.

La protection de la vie privée dans l'univers numérique passe par l'éducation des plus jeunes. Le défi est de trouver un équilibre entre la préservation nécessaire de la liberté sur le Net – car c'est un extraordinaire espace de liberté – et la protection de nos concitoyens contre les dérives.

Chaque pays a sa sensibilité et sa culture sur ces sujets mais c'est par des positions communes que nous pourrons peser.

Car les dérives sont d'autant plus difficiles à maîtriser que les acteurs sont multiples et puissants. Les États semblent parfois démunis face à un phénomène qui ne connaît ni les frontières ni les territoires.

Les États ne peuvent rester impuissants. Notre réunion montre aujourd'hui que nous ne souhaitons pas rester passifs et qu'il est de notre responsabilité d'alerter nos concitoyens, de saisir les instances de l'Union européenne de leurs préoccupations, et de proposer des initiatives pour construire des instruments de régulation et de protection dont nous avons besoin sur le plan international.

Il est important pour notre mission d'information que la révision de la directive communautaire du 24 octobre 1995 relative à la protection des données personnelles qui est annoncée prenne clairement en compte ces préoccupations. Le déplacement que nous avons effectué à Bruxelles en octobre dernier nous a laissé perplexes sur l'engagement des autorités communautaires en ce domaine. Nous devons porter ces questions devant les instances européennes en montrant notre volonté d'être actifs.

C'est aussi au-delà de l'Europe que nous devons nous faire entendre. C'est là, également, un objectif majeur de nos travaux.

Le Président de la République française a évoqué l'organisation d'un G8 de l'Internet, c'est évidemment une initiative heureuse. Face à des grands groupes, par exemple, qui semblent vouloir créer leur propre loi, il est important que les États ensemble rappellent les grands principes des droits individuels.

Pour toutes ses raisons, je suis très heureux que nous puissions engager ce dialogue par-dessus le Rhin, par une voie numérique. Au-delà du symbole, il nous faudra avancer des propositions concrètes. Je crois que Monsieur le président Fischer et nos collègues allemands partagent cet objectif.

M. Axel E. Fischer, président, ***(Bundestag)*** **–** Monsieur le président Jean-Luc Warsmann**,** chers collègues de l'Assemblée nationale, la commission d'enquête du *Bundestag* vous salue depuis Berlin, vous et vos collègues. Nous sommes très heureux de vous retrouver et l'ensemble de notre commission se réjouit de pouvoir envoyer un signal fort par cette visioconférence. Ce signal montrera que les parlements français et allemand se mettent directement d'accord sur des questions importantes concernant la société numérique et qu'ils sont prêts à mettre tout leur poids dans la balance sur ces questions.

Le mandat de notre commission « Internet et la société numérique » est très large. Nous devons passer en revue, pendant deux ans, les conséquences du développement d'Internet dans différents secteurs de notre société – en particulier dans les domaines de l'économie, de la culture, de l'éducation et des médias – et voir où il est nécessaire d'agir. A la fin de notre travail nous formulerons des recommandations à l'intention du *Bundestag*. Celles-ci pourront porter sur le droit national mais aussi sur des initiatives internationales. Il est possible aussi que dans certains cas on recommande qu'il ne soit pas introduit de législation nouvelle.

Au-delà de l'agenda politique du moment, nous tentons de rendre compte de la gigantesque dynamique sociale, économique et culturelle d'Internet et cherchons à aller au fondement de ce phénomène. Nous organisons des auditions publiques et nous discutons à l'intérieur et à l'extérieur de la commission avec de très nombreux acteurs de ce champ politique relativement récent.

Notre commission compte 34 membres, dont neuf participent à notre débat d'aujourd'hui. Sa composition est particulière puisqu'elle est formée pour moitié de députés et pour moitié de spécialistes non parlementaires provenant de différents secteurs : science, monde des entreprises, associations et médias. Ceux-ci donnent une véritable impulsion à notre réflexion en nous permettant de mieux cerner les problématiques spécifiques de l'Internet et de sortir de nos schémas de pensée habituels.

Nos travaux ont débuté le 5 mai 2010. Cinq groupes de travail ont été créés : sur la neutralité du Net, les droits d'auteur, l'apprentissage aux bonnes

pratiques des médias et sur les sujets débattus aujourd'hui, à savoir les données personnelles et les droits de la personne.

Nous avons prévu, pour cette année, la création de huit groupes de travail supplémentaires qui traiteront, entre autres, de la gouvernance d'Internet dans le contexte international, d'Internet dans le monde de l'entreprise et du travail ainsi que des rapports de l'État et de la démocratie à l'ère d'Internet.

J'espère qu'en quelques mots j'aurai pu vous donner une idée de ce que sont nos travaux. Nous aurons, par la suite l'occasion d'approfondir tel ou tel aspect, ou de poser des questions et d'y répondre.

Après Pâques, nous présenterons un rapport intermédiaire et l'an prochain le rapport final sera adopté par le *Bundestag*.

Le sujet qui est l'objet de notre débat d'aujourd'hui, à savoir les données personnelles et les droits de l'individu, a été structuré en cinq thématiques. Deux députés à Paris et deux députés à Berlin interviendront sur chaque thème. Nous nous sommes mis d'accord pour fixer à 3 minutes le temps de parole de chaque intervenant pour que tous les députés puissent s'exprimer. Le premier thème abordé sera celui de la protection de la vie privée sur Internet.

Thème 1 : Protection de la vie privée sur Internet

M. Jean-Luc Warsmann, président, *(Assemblée nationale)* – Lors des travaux de notre mission, nous avons été frappés par le fait que de plus en plus de nos concitoyens exposent leur vie privée sur Internet, notamment les plus jeunes, et qu'ils le font sans en avoir toujours conscience. Quand ils en prennent conscience et souhaitent mieux protéger leurs droits, ces internautes sont confrontés à des difficultés techniques et juridiques.

Avec le développement des réseaux numériques fixes et mobiles et, plus largement, des nouvelles technologies de l'information et de la communication, le débat sur la protection de la vie privée est sorti du monde des experts pour devenir une question qui se pose à chacun.

La France avait été précurseur en la matière voilà plus de trente ans. En effet, le respect de la vie privée passe d'abord par la manière dont sont collectées, exploitées et conservées les données personnelles par les entreprises, les administrations et les individus eux-mêmes. La France a adopté, en 1978, une loi fondatrice – la loi « Informatique et libertés » – qui est la pierre angulaire de la protection des citoyens face aux traitements de données à caractère personnel.

Ce cadre juridique a devancé et, parfois même, inspiré, la mise en place de règles au niveau international et européen, comme la directive du 24 octobre 1995 sur la protection des données personnelles.

Mais il nous semble aujourd'hui nécessaire et indispensable d'évaluer, par rapport aux évolutions technologiques ininterrompues de ces dernières années, la pertinence de ces règles de protection de la vie privée. Une approche commune avec nos partenaires européens est évidemment fondamentale en particulier dans le cadre de la révision de la directive de 1995.

M. Axel E. Fischer, président, *(Bundestag)* – Nous estimons également qu'il faut prendre très au sérieux les préoccupations de nos concitoyens sur ces questions.

M. Jens Koeppen, *(Bundestag)* Membre du *Bundestag* depuis 2005, je suis spécialiste en électrotechnique et entrepreneur. J'ai grandi dans un pays qui ne connaissait pas la liberté – la République démocratique allemande – et je sais par conséquent ce que signifie un libre accès à la connaissance, ce dont nous étions privés à l'époque. C'est pourquoi Internet est, selon moi, le réseau de communication et d'information le plus libre du monde. Au sein de cette commission d'enquête je m'efforce d'aider au développement de ce réseau et de m'opposer aux détournements dont il peut faire l'objet. Internet doit être utilisé pour le bien de tous. Il ne faut pas dire qu'il présente trop de risques et que derrière chaque internaute se cache un danger. Il convient de faire preuve de prudence. La France et l'Allemagne ont déjà un niveau de protection très élevé et il ne faut pas tomber dans un interventionnisme effréné. Un de nos ministres a d'ailleurs très sensément affirmé, récemment, qu'il convenait, certes, de lutter contre tous les abus sur Internet, sinon on risquait la mort de cet outil de communication, mais qu'il fallait tracer des limites et dresser des garde-fous avec mesure pour que les utilisateurs et les fournisseurs de service restent libres de leurs actions.

En tant que citoyen je dois également être prudent sur les informations que je mets sur Internet. On ne peut pas toujours se reposer sur l'État. Le citoyen doit être responsabilisé quand il communique des données. Il faut tendre vers un juste équilibre entre ces deux dimensions.

M. Lars Klingbeil, *(Bundestag)* – Nous sommes face à des processus qui vont transformer de manière révolutionnaire notre vie. Je fais partie d'une génération qui utilise en permanence Internet. Membre depuis six mois du *Bundestag*, je suis très engagé sur ces questions au nom du SPD. Les discussions stériles sont à éviter car les opportunités offertes par ces transformations sont très importantes. Ainsi les polémiques dont *Google Street View* a fait l'objet l'an dernier ont pu laisser croire qu'il n'y avait que des aspects négatifs dans ce service. Or cela est faux car de nombreux aspects de *Google Street View* sont à mettre en valeur. Il y a bien sûr des défis à relever ; par exemple l'interconnexion de certaines données peut poser problème.

La protection des données a d'abord consisté à se protéger contre l'État. Aujourd'hui, il faut que les citoyens, avec l'aide de l'État, apprennent à se protéger contre les grandes entreprises.

Le plus grand défi est d'apprendre aux citoyens à se comporter correctement sur Internet. Il faut qu'ils aient conscience des précautions à prendre quand ils utilisent cet outil.

Nous avons une mission politique à remplir. Certes, les niveaux de protection des données en France et en Allemagne sont élevés mais avec l'internationalisation croissante nous sommes confrontés sans cesse à de nouveaux problèmes, par exemple la création de profils d'utilisateurs, la mise en ligne de profils professionnels ou le *tracking* [suivi] de données. Notre coopération franco-allemande pourra donner un signal positif au niveau européen.

En tant qu'Européens nous devons également rechercher un accord avec les États-Unis pour renforcer la protection des données.

M. Patrick Bloche, rapporteur, ***(Assemblée nationale)*** **–** Député de Paris depuis 1997, j'ai créé dès cette date, avec deux collègues, un groupe d'études à l'Assemblée nationale, consacré à Internet. En 1998 j'ai été parlementaire en mission auprès du Premier ministre Lionel Jospin et je participe depuis lors à tous les débats parlementaires portant sur Internet.

Notre mission d'information aborde évidemment Internet en tenant compte de tous les apports positifs de cet outil qui a révolutionné les rapports entre les hommes et renversé les frontières. Dans de nombreux pays dans lesquels les citoyens ne bénéficient pas des mêmes protections qu'en France et en Allemagne, Internet est censuré parce qu'il dérange.

Mais nous avons également le souci de défendre les droits des individus et l'on constate qu'Internet permet, selon certains, de battre en brèche la notion même de vie privée. Un travail de régulation est donc à mener. Nous verrons à la fin de notre mission si cela passe par une nouvelle législation. En ce sens, nous accordons beaucoup de valeur à la solidité du couple franco-allemand en ce domaine et à sa capacité d'initiative telle qu'elle a pu déjà se manifester en particulier en 1995 lors de l'élaboration de la directive sur les données personnelles. Pour la prochaine échéance européenne nous devons être en mesure d'entraîner les autres pays européens et de créer une dynamique plus large, car on sait qu'Internet n'a pas de frontières et que la protection de la vie privée doit pouvoir être assurée en tout point du globe.

Nous avons été frappés au cours de nos auditions du fait que les grands acteurs d'Internet, comme *Facebook* et *Google* sont des interlocuteurs parfaits au niveau du discours et des intentions mais que dans la réalité, pour des raisons commerciales, les internautes ne bénéficient pas des informations nécessaires. Il ne s'agit pas de condamner, par exemple, le ciblage publicitaire en tant que tel mais on constate que les utilisateurs ne sont pas assez informés de l'utilisation qui est faite de leurs données de navigation. Les internautes ne sont pas tous des experts en informatiques et il leur est difficile d'identifier le point de contact nécessaire pour exercer leur droit d'opposition au traitement de leurs données. La

procédure d'*opt-in* permettant de recueillir le consentement *a priori* de l'utilisateur n'est pas proposée aux internautes. Il faut leur apporter des garanties de cette nature.

M. Patrice Verchère, rapporteur, *(Assemblée nationale)* – Député du Rhône depuis 2007, membre de la commission des Lois, j'ai été nommé co-rapporteur de cette mission à la suite de la démission du collègue qui occupait cette fonction. Sans être spécialiste d'Internet, j'ai un regard de citoyen qui se pose beaucoup de questions. Les auditions menées par notre mission ont montré que les informations portant sur la manière d'utiliser Internet font défaut. Il est très important de trouver un équilibre entre la liberté de « donner des données » et le nécessaire droit de regard que leurs possesseurs doivent avoir sur elles, sous la forme par exemple de droit à l'oubli. Des progrès sont à faire en matière de consentement quand des données personnelles sont recueillies à des fins publicitaires. Or le consentement est un élément essentiel pour que le Net reste un espace de liberté, espace dont on a encore pu vérifier l'importance pour la démocratie lors des récents événements en Tunisie.

Je suis persuadé que nous devons travailler en commun sur la révision de la directive européenne de 1995. Le couple franco-allemand peut jouer un rôle essentiel pour parvenir à une solution équilibrée et respectueuse de tous les intervenants.

Thème 2 : Conservation des données et « droit à l'oubli »

M. Axel E. Fischer, président, *(Bundestag)* – Notre ministre en charge de la protection des consommateurs, Madame Ilse Aigner, a avancé l'idée intéressante d'une gomme numérique. Mais avant de s'interroger sur les modalités concrètes d'utilisation de cet outil il convient de répondre au préalable à une question clé : les citoyens peuvent-ils avoir le droit de « disparaître » de certaines pages d'Internet ? Existe-t-il un « droit à l'oubli »?

M. Manuel Höferlin, *(Bundestag)* – Membre du Parlement depuis 2009, j'appartiens à la commission juridique et à la commission de l'intérieur. J'ai été directeur d'une société de conseil en technologies de l'information et de la communication pendant plusieurs années et je me réjouis qu'au *Bundestag* on puisse travailler avec des experts sur ce sujet.

Quand on parle de droit à l'oubli, il convient de se référer en premier lieu à l'utilisateur qui doit apprendre à être responsable lorsqu'il met des données sur Internet et être conscient de ce qu'il fait quand il introduit des informations sur le Web. Cette responsabilisation est une question de compétence dans l'usage des médias, question qui concerne tous les utilisateurs et pas seulement les jeunes. D'un autre côté, le contrôle de l'utilisation des données peut être réalisé par les gestionnaires de réseaux mais dans certaines limites seulement.

Deux aspects sont à considérer. D'abord, la question des réseaux sociaux où, selon le droit allemand, chacun a le droit de demander que soient retirées les

données qu'il y a mises ; encore faut-il que les fournisseurs d'accès procèdent effectivement à l'effacement complet des données en cause et ne se contentent pas d'empêcher la mise en ligne de nouvelles données. À l'occasion d'un téléchargement de données, par exemple d'une photographie, l'autorisation de la personne concernée doit être demandée. Le droit à l'oubli est déterminé par les utilisateurs eux-mêmes.

Mais on connaît, par ailleurs, « l'effet Barbra Streisand » ; cette actrice avait voulu faire retirer d'Internet une photographie qui avait été prise de sa maison sans son autorisation ; sa demande a suscité un tel intérêt dans la communauté des Internautes qu'aujourd'hui il est impossible d'effacer ce document. Plus une information présente un intérêt, plus elle est diffusée sur la Toile et moins il devient possible de l'effacer. *Wikileaks* relève de la même logique.

Pour les réseaux sociaux, le problème est un peu différent. Ce sont surtout des données personnelles et des biographies qui y sont mises en mémoire. On peut se demander s'il ne serait pas nécessaire de contraindre les réseaux sociaux à effacer les données qui ne sont plus utilisées. Toutes les données d'un profil d'utilisateur devraient pouvoir devenir obsolètes après un certain délai si aucun usage n'en est fait. C'est là une idée à laquelle il conviendrait de réfléchir sur le plan international.

Je suis, par contre, beaucoup plus sceptique sur l'idée d'effacer des données qui ne sont pas à l'intérieur d'un réseau social mais sont diffusées sur l'ensemble du Web. Créer une véritable « gomme numérique » me semble très difficile. La version de cette gomme qu'on connaît aujourd'hui en Allemagne n'est d'ailleurs pas véritablement une « gomme » ; il s'agit d'une technique de cryptage des informations dans le temps, applicable, par exemple, aux photographies.

M. Jean-Luc Warsmann, président, ***(Assemblée nationale)*** – La législation française reconnaît d'ores et déjà quatre droits en matière de conservation des données : le droit pour toute personne d'accéder à l'intégralité des données conservées à son sujet ; le droit pour toute personne d'être informée de la mise en œuvre d'un traitement de données personnelles ; le droit pour toute personne de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et de refuser, sans avoir à se justifier, que les données la concernant soient utilisées à des fins de prospection commerciale ; et, enfin, le droit pour toute personne de faire rectifier, compléter, actualiser ou effacer des informations la concernant lorsqu'ont été décelées des erreurs ou des inexactitudes.

Mais il est certain qu'avec Internet et les nouvelles technologies, les capacités de conservation des données se sont démultipliées et les informations restent visibles de façon permanente. Se pose donc la question, au-delà du droit existant, de la reconnaissance d'un véritable « droit à l'oubli » qui permettrait à

toute personne de retirer, en quelque sorte, les informations publiques la concernant et dont elle ne souhaiterait plus permettre la consultation.

M. Marcel Rogemont, ***(Assemblée nationale)*** **–** Député de Rennes, en Bretagne, je salue nos collègues allemands.

Le « droit à l'oubli » est une notion confuse qui peut s'appliquer à diverses catégories d'informations personnelles.

Ce droit peut, en premier lieu, porter sur les données personnelles faisant l'objet d'un traitement. En France la Commission nationale Informatique et libertés garantit en ce sens ce droit à l'oubli, par exemple le droit de rectifier ses données. Les questions qui se posent sont alors de savoir pendant quelle durée maximale ces données peuvent être conservées sur les serveurs et si, à l'issue de ce délai, ces données sont effectivement effacées des supports où elles ont été conservées.

Ces deux questions n'ont pas trouvé de solution satisfaisante et se heurtent à des réticences de la part des acteurs d'Internet. Ainsi, le 13 octobre 2010, une charte portant sur le droit à l'oubli dans les sites collaboratifs et les moteurs de recherche a été signée par plusieurs acteurs de l'Internet à l'instigation du secrétariat d'État à la prospective et au développement de l'économie numérique. Mais *Google* qui représente 65 % des parts de marché des moteurs de recherche et *Facebook* n'ont pas souhaité s'associer à cette démarche d'autorégulation.

En tout état de cause, cette charte engage uniquement ses signataires et reste dépourvue de toute valeur contraignante, puisqu'elle ne prévoit aucune sanction en cas de non-respect de ses dispositions.

En second lieu, peuvent être concernées des informations portant sur la vie personnelle d'un individu. En raison des capacités de mémoire d'Internet, ces données peuvent réapparaître plusieurs années après avoir été mises en ligne et porter préjudice à la personne concernée. Il peut s'agir, par exemple, d'une photographie de jeunesse mise sur *Facebook*, de propos tenus lors d'une discussion sur le réseau ou d'une information de presse relatant des faits anciens qui seraient tombés dans l'oubli mais faciles à extraire grâce à des moteurs de recherche. La question est alors de définir les types d'information dont on serait en droit de demander l'effacement. Peut-on ainsi faire table rase et reconstruire sa biographie ? Que deviendrait alors le droit à l'information ?

Toute information sur Internet pouvant être mémorisée, copiée et diffusée, n'est-ce pas illusoire de tenter de légiférer sur un « droit à l'oubli » pris en ce sens-là ?

Une autre question est celle des droits de la personne face au droit commercial lorsque des données personnelles sont recueillies à des fins publicitaires, par exemple par l'intermédiaire des *smartphones*. Les intérêts des sociétés de publicité peuvent-ils l'emporter sur les droits de la personne ?

M. Sébastien Huyghe, vice président, *(Assemblée nationale)* – Député du Nord, je suis élu depuis 2002. Avec un de mes collègues, je représente, depuis 2007, l'Assemblée nationale au sein de la Commission nationale de l'informatique et des libertés (CNIL) qui est en France l'instance de protection des données personnelles.

Le problème du « droit à l'oubli » est fondamental car chaque individu peut évoluer au cours de sa vie. Le principe du « droit à l'oubli » sous tend ainsi toutes les règles de prescription qui permettent, par exemple, d'effacer les données du casier judiciaire.

Sur le Net, il n'existe, par contre, aucune règle d'effacement. Dans le cadre de mes fonctions à la CNIL je suis fréquemment saisi de cas de jeunes gens qui ont envoyé des données sur Internet et qui en subissent les effets en retour des années plus tard. Il peut s'agir, par exemple, de photographies de fêtes que les jeunes aiment mettre sur *Facebook* et qui se retrouvent dans des dossiers d'embauche.

Se pose également le cas des personnes qui ont été condamnées par la justice. Bien qu'elles aient accompli leur peine et qu'elles se soient acquittées de leur dette envers la société, la mention de leur condamnation demeure sur Internet, dans diverses publications, *ad vitam aeternam*.

L'institution d'un « droit à l'oubli » s'impose en tant que principe de liberté individuelle. La difficulté est qu'à cette fin on ne peut se contenter d'agir au niveau national et qu'une collaboration internationale doit être engagée, comme l'a évoqué l'un de nos collègues allemands.

Une telle initiative doit passer d'abord par l'Europe. Le groupe de l'article 29, qui regroupe les différentes instances des pays européens relatives à la protection des données a formulé des préconisations sur ce sujet. Il devrait en résulter une réglementation européenne.

L'institution au niveau international d'un « droit à l'oubli » dépend cependant des discussions avec les pays anglo-saxons qui ont une conception très différente de la protection des données personnelles.

L'urgence des problèmes impose un très grand travail de formation des jeunes utilisateurs d'Internet. Ceux-ci doivent avoir conscience que les informations qu'ils mettent en ligne ne leur appartiennent plus et peuvent avoir des conséquences désastreuses sur leur avenir.

M. Lars Klingbeil, *(Bundestag)* – Il est important que le droit de correction et d'effacement des données sur Internet soit renforcé. Par exemple, lorsque des conditions contractuelles sont modifiées le consommateur doit avoir la garantie que les anciennes données sont effacées. Mais on ne peut pas non plus modifier de façon excessive le mode de fonctionnement d'Internet. Nous avons affaire à un réseau qui est très libre. La ligne à suivre est celle de l'économie des

données c'est-à-dire l'établissement de règles très précises rendant possible l'effacement des données, problème qui a également son importance pour les entreprises.

Les utilisateurs doivent décider de l'usage qui est fait de leurs données. Les *curriculum vitae* sur Internet doivent, par exemple, être mieux protégés.

Pour autant, il ne faudrait pas bouleverser l'organisation d'Internet et menacer sa liberté.

Thème 3 : Protection des mineurs sur Internet

M. Axel E. Fischer, président, ***(Bundestag)*** – Nous devons nous interroger sur la façon de protéger les mineurs dont la vie privée et la sphère intime s'expriment sur les réseaux sociaux, sans que ces jeunes internautes aient conscience des problèmes que cela pose.

M. Jean-Luc Warsmann, président, ***(Assemblée nationale)*** **–** La législation française comporte des mesures particulières de protection en direction des enfants et des adolescents. Les fournisseurs d'accès à Internet sont, par exemple, contraints de fournir gratuitement à tous leurs clients un système de contrôle parental.

La France envisage actuellement, comme l'ont fait des pays tels que le Royaume-Uni, la Norvège ou la Suède, d'obliger les fournisseurs d'accès à Internet à bloquer l'accès aux sites pédopornographiques.

Mais les travaux de notre mission montrent que cette protection doit être renforcée, notamment par la prévention, c'est-à-dire l'éducation aux médias, qui exige un effort de formation et de sensibilisation des mineurs, mais aussi des enseignants et des parents.

M. Patrice Verchère, rapporteur, ***(Assemblée nationale)*** **–** Les mineurs sont particulièrement concernés par la problématique de la vie privée et des données personnelles dans la mesure où ils exposent leur vie intime sur les réseaux sociaux sans être toujours conscients de conséquences que cela peut entraîner.

Notre mission d'information a constaté que les réseaux sociaux ne contrôlaient pas suffisamment l'âge que les mineurs déclarent quand ils s'inscrivent. Il semble donc nécessaire de trouver le moyen de contraindre ces acteurs d'appliquer strictement l'interdiction de s'inscrire avant un certain âge. Mais comment vérifier l'âge de l'utilisateur ? C'est une des difficultés que pose Internet.

Concernant l'éducation aux médias, il se trouve que j'ai rendu un rapport, il y a un an et demi, qui constatait l'existence sur Internet d'un certain nombre de jeux dangereux et qui faisait le bilan de l'éducation dispensée aux enfants pour les

mettre en garde contre les dangers d'Internet. En France, les enfants passent un brevet d'initiation à Internet (B2I) ; l'initiative est bonne mais insuffisante car elle ne laisse pas une place suffisante à l'éducation aux dangers d'Internet. Il convient aussi de mieux former les enseignants sur ces questions. De même un effort d'information est à faire en direction des parents sur les avantages et les dangers du Net pour leurs enfants.

Patrick Bloche, rapporteur, ***(Assemblée nationale)*** **–** Internet est un média. La protection des mineurs sur Internet peut donc être abordée à partir de ce qui se fait déjà sur les médias traditionnels tels que la télévision. Les conditions de régulation propres à l'audiovisuel, dont est chargé en France le Conseil supérieur de l'audiovisuel, ont été étendues aux services de média à la demande (SMAD). Faut-il aller plus loin et étendre les compétences de cet organisme à tous les contenus circulant sur Internet, et notamment aux sites de partage de vidéos ? Certains l'envisagent mais nous avons des doutes sur l'efficacité d'une telle extension. Nous aimerions connaître l'état des réflexions menées en Allemagne en ce domaine.

Le souci d'efficacité peut conduire à recourir à des moyens lourds, comme couper l'accès à un site pour empêcher la consultation d'un contenu. Mais une telle mesure est mal acceptée par les internautes car elle remet en cause une liberté fondamentale, garantie par le Constitution en France, qui est la liberté de communication. Un débat récent à l'Assemblée nationale a ainsi montré que s'il y avait un accord unanime pour mieux lutter contre les diffusions des contenus pédopornographiques, des divergences s'étaient exprimées sur les moyens à mettre en œuvre, en particulier sur la possibilité d'habiliter une autorité administrative à contraindre un fournisseur d'accès à bloquer un site ; certains députés, dont je faisais partie, estimaient que l'intervention d'un juge apportait une garantie fondamentale.

Notre souci est l'efficacité mais nous tâtonnons encore. Faire du mineur un citoyen bien éduqué, conscient des risques qu'il encourt est la meilleure solution.

Encore faut-il que les opérateurs de réseau jouent le jeu. Ces derniers nous ont affirmé, la main sur le cœur, qu'il était pour eux exclu d'accepter l'inscription sur les réseaux sociaux des mineurs de moins de treize ans. Or nous connaissons tous dans notre entourage des mineurs de dix ou onze qui se sont inscrits sans difficultés sur ces réseaux, sans qu'il y ait eu d'intervention de la part des opérateurs. Nous ne sommes donc pas naïfs sur ces questions de régulation.

M. Axel E. Fischer, président, ***(Bundestag)*** – Un grand nombre de ces sujets fait également l'objet de très vives discussions en Allemagne.

Mme Constanze Kurz, ***(expert pour la commission d'enquête du Bundestag)*** **–** Je ne suis pas députée, mais experte en informatique à l'Université Humboldt de Berlin et porte-parole du Chaos Computer Club, le plus grand club

de hackers européens. Dans le cadre de ces débats parlementaires, ma fonction est celle d'une technicienne et porte sur la faisabilité des préconisations qui peuvent être faites concernant Internet.

Les données relatives aux enfants et aux adolescents relèvent de deux champs de problématiques : la protection des données et l'apprentissage de l'utilisation des médias.

L'Allemagne a une disposition législative rendant plus difficile l'accès à certains sites mais elle n'est pas encore appliquée.

Il faut tenir compte du fait qu'Internet a beaucoup évolué depuis trois ans. Aujourd'hui des classes entières de très jeunes enfants sont sur des réseaux sociaux, ce qui correspond à autant de données personnelles mises en ligne.

La question se pose de savoir s'il ne faut pas reconnaître des droits différents pour les adultes et pour les enfants comme il en va dans la vie de tous les jours. Par exemple, le législateur doit prendre des initiatives quand il s'agit de profils de données d'enfants. Les membres du groupe de travail consacré à la protection des données sont d'accord pour reconnaître qu'il convient d'établir des règles portant sur l'utilisation des données d'enfants par les entreprises. La question se pose aussi sur l'utilisation qui est faite de ces données par l'État. Quelles données peuvent être mémorisées et stockées par les pouvoirs publics ? Qu'en est-il des données biométriques recueillies même auprès d'enfants de moins de trois ans à l'occasion de l'établissement d'un passeport ?

Les recommandations que nous ferons au législateur nous obligent à anticiper l'avenir, sur une durée de quatre ou cinq ans.

M. Thomas Jarzombek, ***(Bundestag)*** **–** Je préside, au sein de notre commission d'enquête, les groupes de travail sur la protection des mineurs et sur l'apprentissage de l'utilisation des médias. La question du blocage de l'accès est également débattue en Allemagne. La loi existante, qui le permet, n'est pas appliquée car des doutes demeurent, comme en France, sur la compatibilité d'une telle mesure avec les droits fondamentaux.

Pour combattre la pédopornographie, de nombreuses autres mesures sont envisageables. Leur mise en œuvre est nécessaire.

En Allemagne, la protection des mineurs relève de l'État fédéral mais la mise en œuvre des mesures dépend des *Länder*, ce qui ne simplifie pas la procédure et exige une bonne coopération entre les intervenants. Les *Länder* procèdent à ce qu'on appelle « l'autorégulation régulée ». À l'occasion, par exemple, de jeux ou d'émissions, le contrôle est assuré non par l'État mais par des groupes d'experts indépendants qui donnent des autorisations en fonction des tranches d'âge : 6 ans, 12 ans, 16 ans ou 18 ans. Ce contrôle fonctionne très bien : les médias ne portant pas le label correspondant à l'âge des utilisateurs sont interdits de vente. Mais quand on a voulu appliquer le même système à l'Internet –

ce à quoi j'étais personnellement opposé – cela a été, heureusement, un échec. Une sorte de contrat national avait été proposée pour mieux protéger les mineurs sur le Web. Mais cela aurait engendré beaucoup trop de bureaucratie et aurait été disproportionné. Suite à cet échec, de nombreuses consultations sont menées en ce moment.

Pour lutter contre la pédopornographie il faudrait déjà que les jeunes ne puissent pas accéder à ce type de sites à l'occasion d'une recherche non ciblée. Mais vouloir écarter complètement les jeunes des contenus de cette nature n'est pas réalisable.

Concernant la protection des mineurs sur les réseaux sociaux, une technique efficace est le lancement de campagnes d'information à l'aide de la « communication virale »[1]. De telles campagnes ont permis de lancer avec succès des messages d'avertissement envers les jeunes filles qui mettent sur Internet des photos d'elles-mêmes en bikini. Plus de la moitié des utilisateurs a modifié son comportement suite à cette initiative. Les grands acteurs d'Internet devraient se mettre d'accord pour lancer de cette façon des informations ponctuelles.

Thème 4 : Sécurité des données

M. Axel E. Fischer, président, *(Bundestag)* – Nous connaissons en Allemagne, et il en va sûrement de même en France, un grand nombre d'exemples de failles de données. Celles-ci provoquent non seulement des dommages pour les acteurs économiques mais portent également atteinte aux droits des personnes. Nous avons eu le cas en Allemagne de 100 000 données sensibles qui étaient censées n'être accessibles qu'à un nombre réduit de personnes et qui ont été copiées à partir du plus gros réseau social allemand pour être diffusées sur le Net.

La sécurité des données préoccupe de nombreux citoyens de nos deux pays. Mais l'expérience montre que la conscience qu'on a de ce problème apparaît quand il est déjà trop tard. Que peut-on faire ? Quelles mesures peuvent être prises pour protéger les citoyens et pour les informer en cas de fuite de données personnelles ?

Dr. Reinhard Brandl, *(Bundestag)* – Je suis membre du *Bundestag* depuis 2009. J'ai fait ma thèse en informatique, ai travaillé dans diverses entreprises et ai passé deux ans à l'Institut polytechnique de Grenoble. Je suis donc particulièrement ravi de pouvoir participer à cette visioconférence.

Le problème du droit de la protection des données en Allemagne est qu'il n'est pas assez compréhensible et visible. Moi-même, j'ai des difficultés à cerner le problème car très souvent on ne sait pas ce qui fait l'objet d'un règlement et à quel niveau celui-ci intervient. Or on ne peut compter sur un effet de prévention que si les règles sont connues. La situation peut donc être améliorée sur ce point.

---

1 Les messages sont transmis de proche en proche par les utilisateurs. Cette technique est utilisée par le marketing et passe essentiellement par les réseaux sociaux.

Je recommanderais cependant d'éviter de renforcer des règles dont on ne peut pas encore appréhender les conséquences.

Nos règles précisent les modalités selon lesquelles les citoyens concernés par un problème de données doivent être informés. Mais l'objectif n'est pas vraiment atteint. Des entreprises évoluent en effet dans un milieu international et sont confrontées à des règles d'information diverses et nombreuses, ce qui n'est avantageux ni pour le consommateur ni pour l'entreprise. Un tel problème devrait être abordé en commun au niveau européen, en particulier dans le cadre de la directive européenne. Il y a un très grand potentiel de coopération utile dans ce domaine. C'est pourquoi je me réjouis que la France et l'Allemagne aient envoyé un signal en ce sens.

Mme Constanze Kurz, ***(expert pour la commission d'enquête du Bundestag)*** – Ces dernières années, on a compté en Europe d'innombrables cas de problèmes de sécurité. Des mesures sont donc absolument nécessaires. On connaît l'affaire des télécoms en Allemagne et les problèmes qui se sont posés en Grande-Bretagne.

Il convient, en premier lieu, de réguler les obligations d'information des consommateurs concernés.

Il faut également pouvoir établir les responsabilités au niveau international pour que les personnes en cause puissent savoir contre qui se retourner.

On constate, par ailleurs, que les entreprises et les pouvoirs publics n'investissent pas assez dans la sécurité des données. Une régulation pourrait être proposée à ce niveau pour les inciter à augmenter leur part d'investissement dans ce domaine.

On pourrait aussi renforcer les droits des consommateurs pour qu'ils soient informés par les entreprises qui connaissent une fuite de données.

Certes, la sécurité absolue ne peut pas être garantie. On ne peut qu'augmenter la probabilité de sécurité.

Enfin, un effort est nécessaire dans les universités et les écoles pour former des spécialistes compétents en ce domaine.

M. Sébastien Huyghe, vice président, ***(Assemblée nationale)*** **–** On s'aperçoit que nos préoccupations sont très proches. La coopération européenne est, selon nous aussi, indispensable.

Nous nous interrogeons en particulier sur le fait de savoir qui doit notifier les violations de traitements de données à caractère personnel. La liste des entités tenues de notifier les failles de sécurité est difficile à établir pour les organismes privés : faut-il la limiter aux opérateurs et à des catégories restreintes de

professionnels ou faut-il au contraire l'élargir de façon à englober le plus grand nombre d'entreprises ?

N'y a-t-il pas un risque à définir des catégories trop larges au point d'imposer l'obligation de notification à tous les utilisateurs et d'obliger ainsi la personne qui aura égaré son ordinateur portable à notifier l'incident à l'ensemble des personnes figurant dans le carnet d'adresses qui s'y trouvait ?

Le second problème est de savoir à qui notifier l'incident. Faut-il le faire auprès de la CNIL, qui est habilitée à sanctionner, ou faut-il aller plus loin et instaurer une obligation de notification des violations de traitements de données à caractère personnel aux autorités judiciaires, dès lors que ces violations sont constitutives d'infractions ?

Enfin, notre mission s'interroge sur le degré de publicité qu'il faut donner aux violations de la confidentialité de ces traitements. En effet, une transparence excessive risque de porter atteinte à l'image des administrations ou des entreprises concernées par ces failles de sécurité. Mais, à l'inverse, une transparence insuffisante risque de nuire tout autant à leur image auprès des personnes dont les données à caractère personnel ont été affectées. En outre, si les incidents ne font pas l'objet d'une communication minimale, les entités concernées craignent de ne pas bénéficier des moyens de lutter contre ces violations, puisque, dans ce cas, les moyens techniques et financiers nécessaires pour mettre en place une défense ne sont souvent pas attribués.

M. Marcel Rogemont, ***(Assemblée nationale)*** **–** Je remercie mon collègue de la majorité de céder la parole à un député de la minorité montrant par là que ces problèmes dépassent les clivages politiques, et même nos propres frontières.

En 2009, a été créée en France une Agence nationale de sécurité des systèmes d'information. Cette agence est placée sous l'autorité du Premier ministre français et a pour mission d'orienter la stratégie de l'État en matière de sécurité informatique, de réagir au plus tôt en cas d'attaque informatique, et de prévenir ces attaques en proposant aux administrations des produits et des services de confiance, en délivrant des labels et des certifications.

Nos auditions nous ont appris qu'un organisme semblable existerait en Allemagne. Nous serions intéressés d'en savoir un peu plus sur son organisation, sur son fonctionnement et ses besoins.

Il est évident par ailleurs que ces questions doivent faire l'objet d'une coopération européenne en matière de sécurité des données.

Au cours des auditions faites par notre mission, il nous a été dit que le G29, organisme consultatif placé auprès du Parlement européen et chargé de coordonner les autorités de protection des données de l'Union européenne, bénéficiait de moyens insuffisants et que, parmi les cinq experts nommés au sein du groupe de travail chargé d'examiner le contenu de la future directive

européenne sur la protection des données personnelles, quatre étaient américains. Nous avons tous de la considération pour les Américains, mais cela ne devrait pas empêcher de disposer d'experts européens.

Seriez-vous d'avis de réviser le mode et les moyens de fonctionnement du G29 ?

Thème 5 : Cloud computing et protection des données

M. Jean-Luc Warsmann, président, ***(Assemblée nationale)*** **–** Un nombre croissant de données informatiques gérées par les entreprises n'est plus enregistré sur des serveurs qui leur appartiennent mais est hébergé sur des supports localisés dans des pays relevant de législations très « hétérogènes ». Ces serveurs étant mis en réseau, il s'avère difficile de dire, à un instant « *t* », où est stockée telle ou telle donnée.

Cette exportation de données sur le réseau pose des problèmes juridiques complexes car les informations traitées peuvent contenir des données personnelles. Aussi, notre mission d'information s'interroge-t-elle sur les garanties de confidentialité que présentent ces bases. De quel droit relèvent-elles ? Que deviennent-elles quand elles sont l'objet de sous-traitance ?

Par ailleurs le « *cloud computing* » conduit à multiplier la création de *data centers*. On peut s'interroger sur la sécurité qui est assurée dans ces centres.

L'ensemble de ces questions pourrait relever d'une stratégie européenne.

Patrick Bloche, rapporteur, ***(Assemblée nationale)*** – On s'interroge sur l'équilibre à trouver entre la nécessité de préserver la compétitivité de nos entreprises et celle de préserver la sécurité des données personnelles qui sont massivement externalisées dans le cadre du *« cloud computing* ».

Au cours de nos auditions, nous avons entendu de la part d'une personne chargée de la sécurité des systèmes informatiques les plus sensibles de l'État qu'il n'y avait pas sécurisation absolue et que c'était une mission impossible que d'avoir cet objectif. Cela constitue pour nous un motif d'inquiétude.

Ces systèmes devraient proposer des identifiants sécurisés ce qui renvoie à la problématique intéressante de la carte d'identité numérique.

En cas de fuite de données, la difficulté que l'on connaît déjà à l'intérieur de nos frontières pour assurer la bonne information des personnes concernées se voit considérablement augmentée quand est en cause un sous-traitant situé hors de l'Union européenne.

Les entreprises ne seront-elles pas alors amenées à mettre en place, localement, des sauvegardes de sécurité de leurs données de plus en plus coûteuses et à perdre l'avantage qu'elles avaient à externaliser leurs services ?

Faut-il faire confiance aux acteurs économiques pour s'autoréguler ou, du fait qu'il s'agit de la sécurité à l'intérieur de la zone européenne et d'une concurrence accrue avec les autres parties du monde, devons-nous être plus entreprenants ?

M. Patrice Verchère, rapporteur, ***(Assemblée nationale)*** **–** Comment imposer des audits de sécurité aux acteurs du « *cloud computing* » et peut-on se contenter d'une autorégulation ?

Tous les systèmes de sécurisation des bases de données les plus sensibles incluent dans leurs protocoles des audits techniques de sécurité. On pourrait suggérer que toute société procédant à l'exportation de ses données ne puisse le faire qu'avec des partenaires ayant fait l'objet de tels audits. Cela supposerait cependant des systèmes de labellisation internationaux.

Deux voies sont alors ouvertes : soit le marché, soucieux d'inspirer la confiance des différents acteurs, s'autorégule et met en place des chartes de sécurité, soit les législateurs des pays concernés interviennent. La difficulté est qu'une charte ne s'accompagne pas de sanctions et qu'une législation qui ne présente pas de caractère universel entraîne *de facto* une situation déséquilibrée entre les entreprises en raison des coûts que représente la mise en place de systèmes de sécurisation.

Une autre question est celle des sous-traitances en cascades qui caractérisent le « *cloud computing* ». Ces rapports commerciaux fragilisent encore plus la sécurité de ces transferts de données, surtout quand elles ont lieu en dehors de l'Union européenne. Que deviennent ces données si un des contractants fait défaut ? Dans quelles conditions les personnes dont les données personnelles sont ainsi exportées peuvent-elles avoir accès à ces bases ?

Consciente de cette situation, la Commission européenne a fixé de nouvelles clauses contractuelles, en vigueur depuis le 15 mai 2010, permettant d'encadrer les transferts de données à caractère personnel vers des sous-traitants de données établis dans un État n'offrant pas un niveau de protection adéquat.

Cependant on peut s'interroger : ces types de contrat commerciaux offrent-ils des garanties suffisantes aux personnes dont les données sont ainsi exportées ?

Faut-il alors interdire l'exportation de certaines données ? Par exemple, les données biométriques, les données génétiques, les données judiciaires ou les données financières d'une personne peuvent-elles faire l'objet d'une externalisation dans le cadre du « *cloud computing* » ?

M. Jimmy Schultz, ***(Bundestag)*** **–** Je dirige depuis seize ans une entreprise dans le domaine de l'Internet. Député du *Bundestag* depuis 2009, je suis membre de la commission de l'Intérieur.

La question qui se pose toujours pour le « *cloud computing* » est celle des différents niveaux juridiques en cause. C'est la raison pour laquelle ces problèmes doivent être abordés au niveau international. En Europe, le niveau de sécurité des données est mieux assuré que nulle part ailleurs. Cela représente un avantage compétitif. En tant que législateur notre mission consiste non seulement à conserver ce niveau de sécurité mais à le développer. À cette fin, on peut s'appuyer sur le travail fait au niveau européen ; si une régulation du marché n'est pas souhaitable, car il ne faut pas faire obstacle à la circulation des données, des gardes fous sont cependant nécessaires. Il faut ainsi assurer plus de transparence sur le lieu de conservation de nos données et être en mesure de garantir qu'elles sont localisées dans l'espace le plus sûr. Non seulement les entreprises et les citoyens en bénéficieront mais aussi le « site Europe », qui en sera renforcé.

M. Konstantin von Notz, (*Bundestag*) – Le « *cloud computing* » est une question très importante, y compris pour le groupe des Verts dont je fais partie depuis 2009. Elle révèle en effet la nécessité de faire des économies d'énergie dans le monde numérique. Le « *cloud computing* » recèle de véritables potentialités d'amélioration de ce point de vue.

Un vrai problème de sécurité se pose lorsque des données sont exportées à l'étranger et qu'elles sont traitées dans d'autres pays. Il faut proposer des nouvelles approches pour assurer une meilleure sécurité. L'Union européenne a mandaté un groupe de recherche pour savoir comment pourrait être créé un « *trusted cloud* ». Il conviendra d'identifier les sites qui sont mieux adaptés que d'autres pour procéder à un traitement des données. L'Europe dispose, comme il l'a été dit par mon collègue, d'un atout sérieux en ce domaine du fait du haut niveau de sécurité qui y est assuré.

Il serait possible également d'encourager les activités de labellisation. Des accords au niveau européen seraient nécessaires à cette fin ainsi qu'un ancrage au plan international.

Enfin, la révision de la directive européenne relative à la protection des données représenterait une avancée considérable pour mieux ancrer les bonnes pratiques en matière de « *cloud computing* ». Pourrait être pris en compte à cette occasion l'accord de *Safe harbour* ; mais celui-ci n'est pas suffisant et des exigences plus fortes doivent être formulées. Les nouvelles formes, particulièrement complexes, que présente le contrôle des données doivent mieux être prises en compte pour améliorer la situation et pour utiliser toutes les potentialités positives qu'offre, par ailleurs, le « *cloud computing* ».

Conclusions

M. Jean-Luc Warsmann, président, ***(Assemblée nationale)* –** Monsieur le président Fischer, chers collègues du *Bundestag*, je tiens à vous remercier, au nom de tous mes collègues français, pour la réussite de cette première réunion

commune. Les échanges ont été très riches et sont les premiers pas vers une action de plus long terme.

La mission d'information de l'Assemblée nationale est d'accord avec le contenu de la déclaration commune que nous avons conçue ces jours derniers. Cela sera une première sur de tels sujets entre nos deux assemblées. Cette déclaration montre que nous avons bien conscience des extraordinaires potentialités offertes par la révolution numérique. C'est un nouveau continent qui s'ouvre à nos concitoyens avec des possibilités immenses en termes de liberté et de savoir. Mais cette déclaration est aussi un appel à la responsabilité des États et de l'Europe. Les droits des individus bénéficient de la révolution numérique ; il ne faudrait pas que ces progrès considérables soient obscurcis par des atteintes à ces mêmes droits. La liberté ne va pas non plus sans la responsabilité et l'éducation. C'est aussi le sens de notre déclaration commune.

Je vais tout à l'heure adresser cette déclaration au président de la République, M. Nicolas Sarkozy, et au Premier ministre, M. François Fillon.

Monsieur le président Fischer, si vous en êtes d'accord, ainsi que les membres de votre commission, nous pourrions adresser une lettre commune aux commissaires européens en charge de ces questions, Mme Viviane Reding et Mme Neelie Kroes, afin de les informer de cette démarche et engager, en un second temps, notre action en direction de l'Union européenne.

Je vous remercie très sincèrement de cette réunion commune et forme le vœu que ce ne soit que le début d'une coopération dans le domaine stratégique et que nous puissions continuer et amplifier ce travail commun franco-allemand initié aujourd'hui.

M. Axel E. Fischer, président, ***(Bundestag)*** **–** Je vous remercie, Monsieur le président Jean-Luc Warsmann. Nous sommes d'accord sur bien des points et nous ne pouvons que nous réjouir de la façon dont vous avez cerné les problèmes. Nous nous réjouissons de cette initiative commune et de votre proposition de mettre en route de nouveaux processus européens. Nous vous soutiendrons avec plaisir. Il est toujours utile d'arriver à regarder au-delà des frontières nationales et d'élargir son horizon.

Bien des questions abordées aujourd'hui font un consensus entre nos deux parlements. D'autres thèmes sont peut-être plus polémiques au plan politique. Ce qui compte est que nous ne perdions pas de vue les besoins de nos citoyens car l'Internet fait de plus en plus partie de leur vie. L'idée de la convivialité du réseau doit être, sur cette question, prioritaire. Pour les entreprises, pour le monde de la culture et pour la société nous devons trouver des solutions innovantes et praticables afin que l'Internet reste un moteur de développement, un moteur de la dynamique économique dans nos deux pays.

Je crois qu'en organisant cette visioconférence nous avons fait un premier pas en avant. Il y en aura certainement d'autres. Personnellement, je suis très

confiant. Nous parviendrons à avancer sur la voie que nous avons ouverte et nous arriverons à une heureuse conclusion.

Notre déclaration commune est un signe positif. Elle sera le fondement de notre travail commun dans les années à venir. Nous nous engageons en faveur d'une initiative internationale qui réponde de manière adéquate au caractère transfrontalier du monde numérique. Nous voulons renforcer ce forum de communication le plus libre du monde qu'est l'Internet. Mais nous avons aussi à faire face aux dangers qui menacent les droits de l'individu tant au plan international que national et nous devons trouver les instruments adéquats pour mieux les protéger.

Je vous remercie, Monsieur Jean-Luc Warsmann, de votre initiative. Je tiens à remercier également tous vos collègues français et nos collègues allemands pour les points de vue très intéressants qu'ils ont bien voulu faire entendre.

Nous nous réjouissons d'avance de poursuivre notre coopération.

La séance est levée à 17 h 55

ANNEXE N° 2 : DÉCLARATION PARLEMENTAIRE FRANCO-ALLEMANDE DU 19 JANVIER 2011

Mission d'information

sur les droits de l'individu dans la révolution numérique

Deutscher Bundestag

Enquete-Kommission Internet und digitale Gesellschaft

Paris – Berlin

19 janvier 2011

DÉCLARATION COMMUNE

Déclaration commune de la « mission d'information commune sur les droits de l'individu dans la révolution numérique » de l'Assemblée nationale et de la commission d'enquête « Internet et la société numérique » du *Bundestag* (*Enquete-Kommission „Internet und digitale Gesellschaft“*)

Internet et les technologies numériques offrent non seulement de formidables possibilités d'épanouissement à tout un chacun, mais également des opportunités tout à fait nouvelles pour l'évolution démocratique de la collectivité, l'activité économique, l'éducation, la culture et les sciences.

L'utilisation d'Internet et des technologies numériques est indispensable pour pouvoir maîtriser les nombreux défis auxquels les individus se voient désormais confrontés en France et en Allemagne, comme partout ailleurs dans le monde.

En même temps, la commission d'enquête « Internet et la société numérique » (*Enquete-Kommission „Internet und digitale Gesellschaft“*) du *Bundestag* allemand et la « mission d'information commune sur les droits de l'individu dans la révolution numérique » de l'Assemblée nationale y voient un risque possible pour les droits de l'individu, notamment le droit à la protection de la vie privée et le droit fondamental à la protection des données à caractère personnel. Ces risques nouveaux pour les droits individuels découlent des nouvelles possibilités technologiques, mais aussi d'une évolution des pratiques de communication, et pas uniquement chez les jeunes générations. Les réseaux sociaux n'en sont qu'une illustration.

Les membres de la mission d'information française et de la commission d'enquête allemande considèrent qu'il est indispensable que les assemblées et les gouvernements de nos deux pays se consacrent pleinement à ces questions, qu'ils participent activement au niveau européen aux travaux de révision de la directive européenne 95/46/CE, relative à la protection des données et que, dans ce cadre, ils se prononcent conjointement pour un renforcement des droits des citoyens en matière de protection des données. La mission et la commission apprécieraient qu'en l'espèce, il soit également fait référence à la communauté de vues entre les assemblées des deux pays, telle qu'elle est formulée dans la présente déclaration.

La numérisation de nombreux processus dans l'administration, la vie économique et la vie quotidienne des citoyens entraîne une multiplication des traitements de données, de même qu'un accroissement perpétuel des informations stockées. Aussi les citoyens s'interrogent-ils de plus en plus souvent sur la manière dont ils vont pouvoir exercer effectivement leur droit à la libre disposition de leurs données personnelles (ou « droit à l'autodétermination informationnelle » dans les termes de la Loi fondamentale allemande).

Les possibilités croissantes d'interconnexion entre de multiples bases de données, tant dans la sphère publique que privée, constituent, en outre, un risque potentiel pour la protection des droits de la personne. Il est donc impératif de renforcer les droits de l'individu.

Chaque citoyen doit pouvoir exercer et faire respecter ses droits à être informé sur les données le concernant et à pouvoir effacer, bloquer ou contester ces données, et ces droits doivent être facilement applicables et effectifs, y compris dans le cadre d'Internet.

Outre les dispositions réglementaires, des engagements volontaires de la part des parties prenantes peuvent contribuer à rehausser le niveau de protection des données. En outre, les technologies de protection préventive revêtent une importance croissante. Dès le stade de leur développement, les technologies, produits et modèles économiques nouveaux doivent être conçus dans l'optique d'une protection des données. Les prescriptions légales relatives aux technologies de protection doivent être élaborées selon le principe de la neutralité technologique afin de garantir la protection des données au fur et à mesure de l'évolution technologique – y compris sans que le législateur ait à intervenir. La définition d'objectifs de protection peut avoir tout son sens à cet égard. Des procédures comme l'attribution de labels de qualité peuvent donner une impulsion efficace et orienter le marché vers une meilleure protection des données.

Le puissant attrait qu'exerce Internet réside dans sa conception décentralisée, qui sollicite la participation des utilisateurs, notamment pour élaborer des contenus. Cette participation entraîne une responsabilité nouvelle des internautes vis-à-vis d'une utilisation prudente de leurs propres données, mais aussi des données personnelles relatives à des tiers. Il est nécessaire qu'ils soient sensibilisés aux risques potentiels et informés sur les mesures volontaires de protection qui sont utiles. Aucune protection efficace des données ne sera possible sans qu'y soient associés les individus concernés. Un travail d'explication et le nécessaire partage de la connaissance technique avec les usagers constituent, par conséquent, des objectifs majeurs dans toute politique de protection. Renforcer chez chaque individu la conscience qu'il faut protéger les données constitue également une priorité dans toute la société.

Les enfants et les jeunes, en particulier, ont besoin d'être protégés. Il est donc indispensable de proposer aussi une formation spécifique sur ces questions à destination précisément des jeunes.

En tant qu'espace d'interconnexion global en constante expansion, Internet peut considérablement favoriser le développement d'une communauté mondiale. C'est le forum d'information et de communication le plus libre qui soit au monde. Mais cela signifie aussi que les législations nationales, comme également les réglementations européennes, ne peuvent à elles seules réussir à écarter les risques qui pèsent sur les droits de l'individu même si de telles

dispositions, nationales et européennes, peuvent évidemment être nécessaires et efficaces pour protéger les citoyens en ce domaine.

La commission d'enquête du *Bundestag* allemand « Internet et la société numérique » (*Enquete-Kommission „Internet und digitale Gesellschaft“*) et la « mission d'information commune sur la protection des droits de l'individu dans la révolution numérique » estiment toutes deux que l'élaboration d'instruments internationaux, allant au-delà du cadre européen, s'impose afin de permettre de mieux faire respecter la protection des droits de la personne.

Gemeinsame Erklärung der Enquete-Kommission „Internet und digitale Gesellschaft“ und der „Mission d’information commune sur les droits de l’individu dans la révolution numérique“ der Assemblée nationale

Internet und Digitalisierung bieten nicht nur weitreichende Entfaltungsmöglichkeiten für jeden Einzelnen, sondern auch ganz neue Chancen für die demokratische Weiterentwicklung des Gemeinwesens, für die wirtschaftliche Betätigung, Bildung die Kultur und Wissenschaft.

Der Einsatz von Internet und digitalen Techniken ist unerlässlich, um vielen Herausforderungen, mit denen sich die Menschen in Frankreich und Deutschland wie überall sonst auf der Welt gegenwärtig konfrontiert sehen, wirksam zu begegnen.

Gleichzeitig beobachten die Enquete-Kommission des Deutschen Bundestages „Internet und digitale Gesellschaft“ und die „Mission d’information commune sur les droits de l’individu dans la révolution numérique“ der Assemblée nationale ein mögliches Risiko für die Rechte des Einzelnen, insbesondere den Schutz der Privatsphäre und da Grundrecht auf den Schutz personenbezogener Daten. Ausgangspunkt dieser neuen Risiken für individuelle Rechte sind neue technische Möglichkeiten, aber auch ein verändertes Kommunikationsverhalten, nicht nur der jüngeren Generation. Soziale Netzwerke sind hierfür nur ein Beispiel.

Die Mitglieder der französischen Mission d’information und der deutschen Enquete-Kommission halten es für unerlässlich, dass die Parlamente und Regierungen unserer beiden Länder sich voll und ganz diesen Fragen widmen, sich aktiv in den angelaufenen Prozess der Revision der EG-Datenschutzrichtlinie 95/46/EG auf europäischer Ebene einschalten und sich in diesem Rahmen gemeinsam für eine Stärkung der Datenschutzrechte der Bürgerinnen und Bürger einsetzen. Die Kommissionen würden es begrüßen, wenn dabei auch auf das in dieser Erklärung zum Ausdruck gekommene Einvernehmen der Parlamente beider Länder Bezug genommen wird.

Die Digitalisierung vieler Abläufe in Verwaltung, Wirtschaft und im Alltag der Bürger bringt eine Vermehrung von Datenverarbeitungen ebenso mit sich wie ein unaufhörliches Anwachsen von Datenbeständen. Bürgerinnen und Bürger stehen daher immer häufiger vor der Frage, wie sie ihr Recht zur freien Bestimmung über ihre persönlichen Daten (oder „informationelles Selbstbestimmungsrecht“ wie es aus dem deutschen Grundgesetz abgeleitet wird) tatsächlich ausüben sollen.

Die zunehmende Möglichkeit der Vernetzung unterschiedlicher Datenbestände im öffentlichen und privaten Bereich birgt ein Risiko für den Schutz von Persönlichkeitsrechten. Eine Stärkung der Rechte des Einzelnen ist daher geboten.

Rechte der Betroffenen etwa auf Auskunft, Löschung, Sperrung oder Widerspruch müssen in ihrer Ausübung und Durchsetzung bürgerfreundlicher werden und auch im Kontext des Internet einfach handhabbar und realisierbar sein.

Neben rechtlichen Regelungen können Selbstverpflichtungen der beteiligten Branchen zur Verbesserung des Datenschutzniveaus beitragen. Daneben kommt dem präventiven technologischen Datenschutz eine wachsende Bedeutung zu. Bereits im Stadium der Entwicklung sind neue Technologien, Produkte und Geschäftsmodelle auf den Datenschutz hin zu konzipieren. Gesetzliche Vorgaben zum technischen Datenschutz sollten technikneutral ausgestaltet sein, damit der Datenschutz – auch ohne gesetzgeberisches Tätigwerden - bei weiterem technologischem Fortschritt gewährleistet ist. Sinnvoll kann die Formulierung von Schutzzielen sein. Verfahren wie die Verleihung von Gütesiegeln können wirkungsvolle, marktsteuernde Anreize in Richtung auf einen besseren Datenschutz geben.

Die große Attraktivität des Internets beruht auf seiner dezentralen Struktur, die alle Nutzerinnen und Nutzer zum Mitmachen, etwa zur Gestaltung von Inhalten, einlädt. Damit einher geht eine neue Verantwortung der Menschen für einen sorgfältigen Umgang mit eigenen Daten, aber auch mit personenbezogenen Daten Dritter. Erforderlich sind die Sensibilität für mögliche Gefahren und das Wissen darüber, welche Maßnahmen des Selbstschutzes möglich und sinnvoll sind. Wirkungsvoller Datenschutz im Internet ist ohne diesen Beitrag der Betroffenen nicht möglich. Aufklärung und die Weitergabe des technischen Wissens an die Nutzer sind deswegen wichtige datenschutzpolitische Ziele. Die Stärkung des Datenschutzbewusstseins bei jedem Einzelnen ist auch eine gesamtgesellschaftliche Aufgabe.

Kinder und Jugendliche sind in besonderer Weise schutzbedürftig. Ein spezifisches Bildungsangebot im Bereich Datenschutz gerade auch für junge Menschen ist daher unerlässlich.

Als Ort einer ständig fortschreitenden globalen Vernetzung kann das Internet die Entwicklung einer globalen Gemeinschaft erheblich befördern. Es ist das freiheitlichste Informations- und Kommunikationsforum der Welt. Damit einher geht aber auch, dass Risiken der Rechte des Einzelnen in vielen Fällen allein durch nationale Datenschutzgesetze oder auch europaweite Regelungen nicht wirksam begegnet werden kann, wenn solche nationalen und europäischen Regelungen auch zweifelsohne nötig und wirkungsvoll sein können, um die Bürger in diesem Bereich zu schützen.

Die Enquete-Kommission des Deutschen Bundestages "Internet und digitale Gesellschaft" und die "Mission d’information commune sur les droits de l’individu dans la révolution numérique" stimmen darin überein, dass auch die Entwicklung - von über Europa hinausgehenden - internationalen Instrumenten geboten ist, um eine bessere Durchsetzbarkeit des Schutzes der Persönlichkeitsrechte zu erreichen.

ANNEXE 3 : RÉSOLUTION DE MADRID DU 5 NOVEMBRE 2009

Résolution sur l'urgence de protéger la vie privée dans un monde sans frontière etl'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles. Document adopté à Strasbourg, 15-17 octobre 2008.

Auteur de la proposition :

- L'Agencia de Protección de Datos (Espagne) et
- le Préposé fédéral à la protection des données et à la transparence (Suisse)
- Coparrains :
- La Commission nationale de l'Informatique et des Libertés (France)
- Le Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Le Garante per la Protezione dei Dati Personali (Italie)
- L'Inspectorat d'État à la protection des données de la République de Lituanie
- L'Office pour la protection des données de la République Tchèque
- L'Autorité hellénique de protection des données
- L'Autorité néerlandaise de protection des données
- Le Contrôleur européen à la protection des données
- L'Inspecteur général à la protection des données (Pologne)
- Le Commissaire à la protection des données de l'Irlande
- La Direction nationale pour la protection des données de l'Argentine
- L'Agence de protection des données de la Principauté d'Andorre
- L'Office du commissaire à l'information (Royaume Uni)
- La Commission nationale de la protection des données (Portugal)
- Le Commissaire à la vie privée de Nouvelle Zélande
- Le Data Protection Commissioner of Guernsey
- Le Berliner Beauftragte für Datenschutz und Informationsfreiheit
- L'Agence de protection des données du Pays Basque (Espagne)
- L'Agence de protection des données de la Catalogne (Espagne)
- L'Agence de protection des données de Madrid (Espagne)
- La Conférence rappelle que:
- la déclaration adoptée à Venise lors de sa 22e Conférence ;

- la résolution adoptée à Wroclaw lors de sa 26e Conférence ;
- la déclaration adoptée à Montreux lors de sa 27e Conférence ;
- l'initiative de Londres présentée lors de sa 28e Conférence ;
- la résolution adoptée lors de sa 29e Conférence ;
- tendent à renforcer le caractère universel du droit à la protection des données et à la vie privée et appellent au développement d'une Convention universelle pour la protection des personnes à l'égard du traitement des données personnelles.
- En particulier dans la déclaration de Montreux, la Conférence appelle l'Organisation des Nations Unies à préparer un instrument juridique contraignant énonçant en détail le droit à la protection des données et à la vie privée en tant que droits de l'homme exécutoires. La Conférence appelle également le Conseil de l'Europe, conformément à l'article 23 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, à inviter les États non-membres de cette organisation qui ont une législation de protection des données adéquate, à adhérer à la Convention (STE N° 108) et à son protocole additionnel (STE N° 181).
- Dans la résolution de la 29e Conférence, les commissaires ont souligné la nécessité de soutenir l'élaboration de normes internationales de protection de la vie privée effectives et universellement acceptées comme un mécanisme pour aider les parties à établir et à démontrer la conformité avec les exigences légales de protection des données et de la vie privée.

La Conférence relève que des efforts encourageants ont depuis lors été entrepris en vue de réaliser ces objectifs et qu'en particulier

- La question d'une Convention universelle est inscrite au programme de travail de la Commission du droit international des Nations Unies ;
- Le Conseil de l'Europe est favorable à l'adhésion d'États non-membres ayant une législation de protection des données conforme à la Convention STE N° 108 et a décidé de promouvoir l'instrument au niveau mondial ; il a ainsi rappelé la vocation potentiellement universelle de la Convention STE N° 108, notamment lors du Sommet mondial sur la Société de l'information à Tunis en novembre 2005 et dans le cadre des Forums sur la gouvernance de l'Internet à Athènes en 2006 et Rio en 2007;
- L'OCDE a adopté le 12 juin 2007 une recommandation relative à la coopération transfrontière dans l'application des législations protégeant la vie privée qui tend notamment à améliorer les cadres nationaux pour l'application des lois sur la vie privée afin que les autorités nationales puissent mieux coopérer avec les autorités étrangères et à élaborer des mécanismes internationaux efficaces destinés à faciliter la coopération transfrontière pour l'application des lois sur la vie privée ;
- Les conférences régionales de l'Unesco en 2005 (Asie-Pacifique) et 2007 (Europe) soulignent le caractère prioritaire de la protection des données ;
- Les initiatives déployées par le groupe de l'article 29 de l'Union européenne pour faciliter la procédure d'adoption de règles d'entreprises contraignantes (BCR) et le développement de solutions contractuelles régissant l'échange transfrontières de données.
- Les chefs d'États et de Gouvernements de la francophonie se sont engagés à l'issu de leur XIe sommet à Budapest en septembre 2006 à intensifier, sur le plan national, les travaux législatifs et réglementaires nécessaires à l'établissement du droit des personnes à la protection des données et à oeuvrer, sur le plan mondial, en faveur de l'élaboration d'une convention internationale garantissant l'effectivité du droit à la protection des données ;
- L'APEC a adopté en novembre 2004 des principes directeurs de la vie privée pour renforcer la protection de la vie privée et préserver les flux d'information. En septembre 2007, l'APEC a lancé une initiative « vie privée » pour développer le cadre de mise en œuvre afin d'assurer des flux internationaux de données certifiés qui répondent aux besoins des affaires, diminuent les coûts de conformité, offrent aux consommateurs un recours effectif, permettent aux régulateurs d'agir efficacement et minimisent la charge réglementaire ;

- L'Association francophone des autorités de protection des données (AFAPDP) créée à Montréal en marge de la 29e Conférence internationale des commissaires à la protection des données et de la vie privée soutient dans ses objectifs l'élaboration d'une convention universelle et les efforts en vue de l'adhésion à la Convention STE N° 108 d'États non-membres du Conseil de l'Europe ;

- Le réseau ibéro américain de protection des données (RIPD) a adopté une déclaration à l'issue de sa 6e réunion tenue en Colombie en mai 2008 appelant les conférences internationales à la protection des données et à la vie privée à poursuivre, indépendamment de leur appartenance géographique, leurs efforts en vue de l'adoption d'un instrument juridique commun ;

- Les Autorités de protection des données d'Europe central et oriental (APDCO), lors de leur dernière réunion en juin 2008 en Pologne, ont exprimé leur volonté de poursuivre et de renforcer leurs activités au sein de l'APDCO, en particulier d'élaborer des solutions communes et d'assister les nouveaux membres dans la mise en place de leur législation de protection des données.

La Conférence considère que:

- le droit à la protection des données et à la vie privée est un droit fondamental des personnes indépendamment de leur nationalité et de leur domicile ;

- qu'avec l'expansion de la société de l'information, le droit à la protection des données et à la vie privée est une condition indispensable dans une société démocratique pour garantir le respect des droits des personnes, la libre circulation des informations et une économie de marché ouverte ;

- la globalisation des échanges et des traitements de données personnelles, la complexité des systèmes, les dommages pouvant découler d'une mauvaise utilisation de technologies de plus en plus puissantes et l'augmentation des mesures sécuritaires nécessitent une réponse rapide et adéquate pour garantir le respect des droits et libertés fondamentales et notamment le droit à la vie privée;

- les disparités persistantes en matière de protection des données et de respect de la vie privée à travers le monde, notamment du fait de l'absence de garantie dans plusieurs États, nuit aux échanges de données personnelles et à la mise en place d'une protection des données effective et globale ;

- le développement de règles internationales qui garantissent d'une façon uniforme le respect de la protection des données et de la vie privée est prioritaire ;

- la reconnaissance de ces droits passe par l'adoption d'un instrument juridique universel contraignant consacrant, recensant et complétant les principes communs de protection des données et de respect de la vie privée énoncés dans différents instruments existants et renforçant la coopération internationale entre autorités de protection des données ;

- La mise en œuvre de lignes directrices développées par des organisations comme l'APEC ou l'OCDE, en particulier celles concernant l'adoption d'un cadre international en vue d'améliorer le respect des droits à la protection des données et à la vie privée lors de flux transfrontières de données est une étape positive pour atteindre cet objectif;

- L'accession à des instruments contraignants de valeur universelle, tel que la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE N° 108) et son protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données (STE N° 181), lesquels contiennent des principes de base de la protection des données, est susceptible de faciliter les échanges de données entre Parties ; ces instruments, en effet, prévoient des mécanismes et une plateforme de coopération entre autorités de protection des données, envisagent l'établissement de ces autorités de manière à exercer leurs fonctions en toute indépendance et favorisent la mise en place d'un niveau de protection des données adéquat;

- la 30e Conférence internationale de la protection des données est une instance appropriée pour adopter une stratégie visant spécifiquement à la réalisation de ces objectifs.

Par conséquent, la Conférence renouvelle son appel d'élaborer un instrument juridique universel contraignant en matière de protection des données et à la vie privée, en adoptant les résolutions suivantes :

- **La Conférence soutient** les efforts du Conseil de l'Europe pour promouvoir le droit fondamental à la protection des données et à la vie privée. Dès lors, la Conférence invite les États membres de cette organisation qui ne l'ont pas encore fait à examiner la ratification de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de son protocole additionnel ; La Conférence invite les États non-membres en position de le faire à considérer de donner suite à l'invitation du Conseil de l'Europe d'accéder à la Convention STE N° 108 et à son protocole additionnel. Considérant sa résolution sur l'établissement d'un groupe directeur relatif à la représentation aux réunions d'organisations internationales, la Conférence souhaite également contribuer aux travaux du comité consultatif de la Convention STE N° 108.

- **La Conférence soutient les initiatives** de l'APEC, de l'OCDE et d'autres organisations régionales et forums internationaux pour le développement de moyens effectifs de promouvoir de meilleurs standards internationaux de protection des données et de la vie privée.

- **La Conférence charge** un groupe de travail, coordonné par l'autorité organisatrice de la 31e Conférence internationale et composé des autorités nationales de protection des données intéressées de rédiger et de soumettre à sa session fermée **une proposition commune d'établissement de normes internationales sur la vie privée et la protection des données personnelles** , selon les critères suivants :

    - de recenser les principes et les droits relatifs à la protection des données à caractère personnel dans les différents environnements géographiques du monde, en faisant en particulier référence aux textes légaux ou autres qui ont rencontré un large degré de consensus dans les forums régionaux et internationaux

    - d'élaborer un ensemble de principes et de droits qui, en reflétant et en complétant les textes existants, permet d'atteindre un degré maximum d'acceptation internationale assurant un haut niveau de protection ;

    - évaluer les secteurs dans lesquels ces droits et principes sont applicables, y compris les variantes qui mettent l'accent sur l'harmonisation de leurs champs d'application ;

    - définir, en tenant compte de la diversité des systèmes juridiques, les critères de base qui garantissent leur application effective ;

    - examiner le rôle que doit jouer l'auto-régulation ;

    - formuler des garanties essentielles pour des transferts internationaux de données meilleurs et plus souples.

Le processus de rédaction de cette proposition conjointe doit être effectué en encourageant une large participation aux groupes de travail et à des forums ou des auditions, des organisations et entités publiques ou privées, en vue d'obtenir le plus large consensus institutionnel et social. Une attention particulière devrait être accordée aux travaux en cours de l'Organisation internationale de normalisation (ISO) et de la Commission du droit international.