N° 4326

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 7 février 2012.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES EUROPÉENNES[1]
SUR LA PROPOSITION DE RESOLUTION EUROPEENNE (n° 4195)
DE PATRICK BLOCHE ET LES MEMBRES DU GROUPE SOCIALISTE, RADICAL, CITOYEN ET DIVERS GAUCHE ET APPARENTÉS
relative **à la protection des personnes physiques à l'égard du traitement des données à caractère personnel au sein de l'Union européenne, notamment dans le cadre de la réforme de la directive 95/46/CE,**

ET PRÉSENTÉ

PAR M. Patrick BLOCHE,

Député

[1] *La composition de cette Commission figure au verso de la présente page.*

La Commission des affaires européennes est composée de : M. Pierre Lequiller, *président* ; MM. Michel Herbillon, Jérôme Lambert, Didier Quentin, Gérard Voisin *vice-présidents* ; M. Jacques Desallangre, M^me^ Marietta Karamanli, MM. Francis Vercamer *secrétaires ;* M. Alfred Almont, M. Patrick Bloche, M^me^ Monique Boulestin, MM. Pierre Bourguignon, Yves Bur, Patrice Calméjane, Christophe Caresche, Philippe Cochet, Jean-Yves Cousin, Bernard Deflesselles, Lucien Degauchy, Michel Diefenbacher, Jean Dionis du Séjour, Marc Dolez, Daniel Fasquelle, Pierre Forgues, M^me^ Marie-Louise Fort, MM. Jean-Claude Fruteau, Jean Gaubert, Hervé Gaymard, Guy Geoffroy, M^mes^ Annick Girardin, M. Philippe Gosselin, Anne Grommerch, Pascale Gruny, Elisabeth Guigou, Danièle Hoffman-Rispal, MM. Régis Juanico, Robert Lecou, Michel Lefait, Lionnel Luca, Philippe Armand Martin, Jean-Claude Mignon, Pierre-Alain Muet, Jacques Myard, Michel Piron, Valérie Rosso-Debord, Odile Saugues, MM. André Schneider, Philippe Tourtelier.

SOMMAIRE

Pages

INTRODUCTION 5

I. LA NECESSITE D'UNE NOUVELLE REGLEMENTATION EUROPEENNE 7

A. LES INSUFFISANCES DE LA DIRECTIVE DU 24 OCTOBRE 1995 8

B. L'ABSENCE D'UN INSTRUMENT JURIDIQUE INTERNATIONAL 12

II. POUR UNE RÉFORME AMBITIEUSE QUI GARANTISSE UN NIVEAU ÉLEVÉ DE PROTECTION 15

A. RENFORCER LES DROITS DES PERSONNES 15

1. Pour une redéfinition du consentement et du droit à l'information 15

2. Imposer de nouveaux droits : droit à l'oubli et droit à la portabilité des données 16

B. DU CÔTÉ DES ENTREPRISES : ENTRE ALLÉGEMENT DES CHARGES ADMINISTRATIVES ET EXIGENCES DE PROTECTION ACCRUES 18

C. PRÉSERVER LES CAPACITÉS D'ACTION DES AUTORITÉS DE PROTECTION DES DONNÉES 20

D. COMPLÉTER LA PROPOSITION DE RÈGLEMENT 21

CONCLUSION 25

TRAVAUX DE LA COMMISSION 27

ANNEXE 1 : PROPOSITION DE RESOLUTION 37

ANNEXE 2 : DÉCLARATION PARLEMENTAIRE FRANCO-ALLEMANDE DU 19 JANVIER 2011 43

ANNEXE 3 : MISSION D'INFORMATION « RÉVOLUTION NUMÉRIQUE ET DROITS DE L'INDIVIDU : POUR UN CITOYEN LIBRE ET INFORMÉ » 47

Mesdames, Messieurs,

Les évolutions technologiques de la dernière décennie ont créé de nouvelles opportunités d'échanger et d'accéder à l'information.

Ainsi, le développement d'Internet s'est accompagné de l'explosion des réseaux sociaux. Le web est entré dans la vie quotidienne de chacun multipliant ainsi les occasions de faire apparaître ou de transmettre ses données personnelles. La vie privée des personnes – englobant leur réseau d'amis, leurs idées politiques, leur orientation sexuelle ou encore leur religion – est potentiellement visible instantanément par tous et partout via ces sites de socialisation. Pourtant, tous ne sont pas conscients qu'une telle exposition publique de soi risque d'entraîner une perte de contrôle de ses données personnelles.

Par ailleurs, les systèmes de géolocalisation ouvrent un éventail de services tout en possédant un revers qui est de rendre transparents les déplacements de chacun via son téléphone portable, son titre de transport ou de paiement ou encore par l'usage du télépéage. D'autres outils, comme la vidéoprotection ou la biométrie, se sont imposés. Ces technologies partagent un point commun : l'accroissement de la traçabilité des individus et les risques inhérents en matière de respect de la vie privée.

La protection des données personnelles constitue un véritable enjeu juridique et sociétal, mais également économique tant celles-ci sont devenues l'or noir de l'économie numérique. La gratuité des services offerts dans l'environnement en ligne a, de plus en plus souvent, pour contrepartie la collecte, l'usage et le transfert de ces données. Celles-ci font l'objet d'une commercialisation et sont utilisées afin de constituer les profils des utilisateurs-consommateurs, sans aucune information de ces derniers. L'autorégulation ne peut suffire en la matière, c'est pourquoi il convient, par des règles juridiques, de responsabiliser les entreprises.

L'objectif général ne peut être de contrer les changements fondamentaux en cours en matière de service, de communication, d'échange et d'accès à l'information, mais de les accompagner et de les sécuriser. La France, à travers notamment le travail de la CNIL, a imposé un contrôle strict de la captation, du transfert, de l'utilisation et de la conservation des données à

caractère personnel. Selon leur « sensibilité », ces données font l'objet d'une protection plus ou moins forte.

L'adoption, il y a dix-sept ans, de la directive européenne 95/46/CE 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 fut l'acte fondateur de la protection de la vie privée à l'échelle communautaire. Sa modernisation semble désormais à la fois urgente et indispensable. Dans le cadre de sa prochaine révision, le Parlement français se doit de faire valoir un certain nombre de principes, valeurs et droits essentiels.

En effet, l'ambition de l'Union européenne est de permettre une meilleure circulation des données à caractère personnel en son sein. Néanmoins, un tel objectif ne peut être mené qu'à la seule et unique condition que toutes les garanties soient prises en matière de protection de celles-ci.

Par conséquent, il est nécessaire d'affirmer un certain nombre de principes afin que tous les résidents, français et européens, puissent tirer profit de cette révolution technologique. La protection de la vie privée, et plus globalement de toutes les données personnelles, doit devenir une exigence de fait et de droit au niveau national, mais aussi communautaire et international.

I. LA NECESSITE D'UNE NOUVELLE REGLEMENTATION EUROPEENNE

A l'heure actuelle, la protection des données au sein de l'Union, hormis pour les questions qui relèvent de la politique européenne de sécurité et de défense et de la coopération policière et judiciaire pénale, relève de la directive 95/46/CE du 24 octobre 1995[(2)]. Cette directive vise à la fois à ce que les données à caractère personnel puissent circuler librement entre les Etats membres afin de permettre le bon fonctionnement du marché intérieur et, dans le même temps, à ce qu'un niveau élevé de protection des droits des personnes concernées soit assuré. La directive de 1995 a été conçue comme le cadre juridique général de l'Union.

Il convient de relever que la directive a été élaborée alors que l'utilisation d'Internet était encore balbutiante. L'évolution technologique rapide de ces quinze dernières années, couplée à la mondialisation des échanges de données, nécessite de revoir en profondeur le droit applicable. Les défis posés sont inédits et ne trouvent pas de réponse dans l'environnement juridique actuel. Chacun est aujourd'hui amené à mettre en ligne des données personnelles et à rendre publics de nombreux éléments qui attisent notamment les convoitises commerciales. Les sites de socialisation en sont l'exemple le plus frappant. L'essor de « l'informatique en nuage » (*cloud computing*), qui permet de stocker de grandes masses de données sur des serveurs lointains, pose des questions sensibles de droit applicable et de perte de contrôle sur les informations transmises.

Il faut également souligner l'essor de l'utilisation d'outils relativement sophistiqués qui permettent aux entreprises de mieux connaître les habitudes et le comportement des internautes. Enfin, les outils de localisation géographique se banalisent, sans que l'on mesure toujours bien leur impact en terme de protection des données personnelles.

Au niveau européen, l'entrée en vigueur du traité de Lisbonne a profondément modifié la donne. En effet, le traité donne force juridique contraignante à la charte européenne des droits fondamentaux qui dispose, en son article 8, que « *toute personne a droit à la protection des données à caractère personnel la concernant* ». Ce droit nouveau s'impose donc désormais au sein de l'Union. Les données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne ou d'un fondement légitime et

---

[(2)] 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.

législatif. Toute personne doit avoir le droit d'accéder aux données collectées qui la concernent et d'en obtenir la rectification. Une autorité de contrôle indépendante doit veiller au respect de ces règles.

En outre, l'article 16 du traité sur le fonctionnement de l'Union européenne dispose, lui aussi, que « *toute personne a droit à la protection des données à caractère personnel la concernant* ». Il appartient au Parlement européen et au Conseil, statuant conformément à la procédure législative ordinaire (majorité qualifiée au Conseil et co-décision), d'adopter les règles relatives à la protection des personnes à l'égard du traitement de leurs données personnelles et à la libre circulation de ces données.

A. Les insuffisances de la directive du 24 octobre 1995

La directive définit les données à caractère personnel comme toute information concernant une personne identifiée ou identifiable. La directive ne vise pas le traitement des données personnelles effectué par une personne à des fins exclusivement personnelles ou domestiques. La question du droit national applicable n'est pas totalement réglée par la directive car elle prévoit que chaque Etat applique son droit lorsque le traitement est effectué par un établissement situé sur son territoire (ou en un lieu où sa loi s'applique en vertu du droit international public) et lorsque le responsable du traitement recourt à des moyens de traitement qui sont situés sur son territoire.

Le rapport d'information n° 3560 « *Révolution numérique et droits de l'individu : pour un citoyen libre et informé* », du rapporteur et de M. Patrice Verchère, a bien démontré l'acuité avec laquelle la question du droit applicable se pose. Le principe d'extraterritorialité fait en principe obstacle à l'application d'une législation nationale à l'encontre d'un acteur d'Internet basé à l'étranger. Ainsi, en 2008[(3)], le tribunal de grande instance de Paris a-t-il rappelé que l'article 4 de la directive de 1995 écarte son applicabilité aux traitements dont les responsables sont situés en dehors de l'Union, quand bien même le public visé serait bien européen. Toutefois, des interprétations divergentes ne sont pas à exclure. Par ailleurs, des tribunaux se sont déjà fondés sur le fait qu'un responsable du traitement, sans être établi sur le territoire français ou communautaire, recourre à des moyens de traitement situés sur le territoire français pour lui appliquer le droit français.

Le rapport précise, s'agissant de la société Google, en page 183 :

« *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*

---

(3) Tribunal de grande instance de Paris Ordonnance de référé 14 avril 2008 - Bénédicte S contre Google Inc.,Google France.

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. »

Très nettement inspirée du droit français avec la loi Informatique et libertés de 1978, la directive dispose, en son article 6, que les données personnelles doivent être traitées loyalement et licitement, pour des finalités déterminées, explicites et légitimes. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités de la collecte, exactes et, si nécessaire, mises à jour. La durée de conservation des données personnelles doit être strictement limitée au temps nécessaire à la réalisation des finalités poursuivies. Le principe du consentement de la personne comme préalable au traitement est posé par l'article 7. Cependant, dans un certain nombre de cas, le

consentement n'est pas nécessaire (exécution d'un contrat auquel la personne concernée est partie, obligation légale du responsable du traitement, ou encore sauvegarde de l'intérêt vital de la personne).

Les données dites sensibles ne peuvent en principe pas être traitées. Elles sont définies comme les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle. Toutefois, des dérogations sont prévues (consentement explicite de la personne, législation applicable en matière de droit du travail, défense des intérêts vitaux d'une personne, cas particulier des associations ou fondations à finalité politique ou religieuse par exemple, données manifestement rendues publiques par la personne elle-même). Un certain nombre d'autres dérogations sont prévues en matière de santé, ou encore afin de garantir la liberté d'expression en matière de journalisme ou de littérature.

La personne concernée doit bénéficier d'une information lui permettant de connaître l'identité du responsable du traitement, les finalités du traitement, les destinataires des données, le caractère obligatoire ou non de ses réponses et l'existence d'un droit d'accès et de rectification si les données sont erronées.

En effet, la personne concernée doit disposer d'un droit d'accès sans contrainte et sans délai ou frais excessifs. Elle a également un droit de rectification, d'effacement ou de verrouillage des données si leur traitement n'est pas conforme à la directive. Le droit d'opposition de la personne est plus limité et ne lui permet de s'opposer à un traitement que pour des raisons prépondérantes et légitimes tenant à sa situation particulière. Elle dispose également d'un droit général d'opposition lorsque le traitement est réalisé à des fins de prospection. Toute personne doit également bénéficier d'un droit de recours juridictionnel en cas de violation de ses droits.

Il appartient au responsable du traitement d'assurer la confidentialité et la sécurité du traitement.

La directive impose en outre une obligation de notification préalablement à la mise en œuvre d'un traitement automatisé de données. Tant les entreprises que les autorités de protection des données jugent cette obligation à la fois excessivement lourde et peu opérationnelle en termes de protection des données, étant entendu qu'il n'est pas possible de contrôler effectivement l'ensemble des traitements déclarés.

Les transferts de données vers des pays tiers ne sont en principe possibles que si la Commission européenne a constaté le caractère adéquat du niveau de protection assuré dans ce pays ou si un Etat membre juge que le responsable du traitement offre des garanties suffisantes, notamment par des clauses contractuelles appropriées ou encore lorsque la Commission européenne décide que certaines clauses contractuelles type présentent des garanties

suffisantes. Un certain nombre d'autres dérogations sont également prévues lorsque la personne a indubitablement donné son consentement ou encore pour permettre l'exécution d'un contrat conclu dans son intérêt.

Chaque Etat membre doit prévoir qu'une autorité de contrôle est chargée de surveiller l'application de la directive sur son territoire. Une telle autorité doit disposer de pouvoirs d'investigation, d'intervention et du pouvoir d'ester en justice ou au moins de pouvoir porter d'éventuelles violations à la connaissance d'une autorité judiciaire.

Le cadre juridique que constitue la directive du 24 octobre 1995 est complété par des instruments sectoriels garantissant spécifiquement le respect de la vie privée en matière de communications électroniques. La directive 2002/58/CE du 12 juillet 2002 dite directive « vie privée et communications électroniques »[(4)], 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. Le rapport sur la révolution numérique rappelle que « *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 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* »[(5)].

Puis, devant le caractère très hétérogène des législations adoptées par les Etats membres s'agissant des obligations de conservation des données et de leur durée de conservation par les opérateurs, afin que celles-ci soient disponibles pour les autorités policières et judiciaires à des fins répressives, une nouvelle directive a dû être adoptée afin de limiter les entraves au marché intérieur découlant des obligations différentes qui s'imposaient aux opérateurs, en fonction du pays concerné[(6)]. La directive du 12 juillet 2002 a également été modifiée par la

---

[(4)] 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.

[(5)] Page 166.

[(6)] 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.

directive 2009/136/CE[7] qui 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 (destruction, altération, transmission notamment). L'information relative à l'installation sur les ordinateurs personnels de « *cookies* » est également renforcée.

B. L'absence d'un instrument juridique international

Au-delà de la seule Union européenne, il faut également souligner l'existence de la convention n° 108 du Conseil de l'Europe, signée à Strasbourg le 28 janvier 1981, et son protocole additionnel du 8 novembre 2001, relatifs à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. La convention est, dans les principes qu'elle pose, très inspirée du droit français. En outre, l'article 8 de la convention européenne des droits de l'homme institue le droit au respect de la vie privée et familiale. La Cour européenne des droits de l'homme a rappelé que la protection des données à caractère personnel constitue un élément majeur du respect du droit à la vie privée. 41 Etats, parmi lesquels les 27 Etats membres de l'Union sont parties à la convention 108, qui a force juridique contraignante.

Le rapport d'information sur la révolution numérique et les droits de l'individu précité a rappelé que tout reste à inventer s'agissant d'un cadre juridique international contraignant en la matière. La mission a notamment organisé, le 19 janvier 2011, une réunion commune avec la commission d'enquête du Bundestag allemand sur « Internet et la société numérique ». Une déclaration commune a ensuite été adoptée par la mission d'information et la commission d'enquête qui estiment toutes deux « *que l'élaboration d'instruments internationaux, allant au-delà du cadre européen, s'imposent afin de permettre de mieux faire respecter la protection des droits de la personne* ». Les travaux internationaux des autorités de protection des données doivent également être rappelés. Ainsi, la résolution de Madrid, adoptée par près de 80 autorités de protection des données, le 5 novembre 2009, lors de la conférence internationale des autorités de protection de la vie privée, permet une première ébauche des standards internationaux de protection des données. La résolution rappelle les travaux du Conseil de l'Europe et des autres instances internationales et souligne le caractère fondamental du droit à la protection des données et du droit à la vie

---

[7] 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.

privée. Un instrument juridique universel et contraignant doit consacrer, recenser et compléter les principes communs de protection existants.

Ainsi, la recommandation n° 32 de la mission d'information sur la révolution numérique vise-t-elle 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. »

II. POUR UNE RÉFORME AMBITIEUSE QUI GARANTISSE UN NIVEAU ÉLEVÉ DE PROTECTION

Il convient, à titre préliminaire, de souligner que la Commission européenne a proposé un règlement, en remplacement de la directive de 1995, qui serait donc d'application directe et ne nécessiterait pas de transposition. Une réelle harmonisation des droits nationaux est ainsi visée.

A. Renforcer les droits des personnes

1. Pour une redéfinition du consentement et du droit à l'information

La Commission européenne propose de redéfinir le consentement de la personne concernée comme toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne accepte, par une déclaration ou par un acte positif univoque, que des données personnelles la concernant fassent l'objet d'un traitement. Il appartiendrait au responsable du traitement de prouver qu'une personne a bien consenti au traitement. Il ne pourrait donc y avoir de consentement tacite.

En ce qui concerne le recueil du consentement d'une personne de moins de 13 ans, le consentement devrait être donné ou autorisé par un parent de l'enfant ou par une personne qui en a la garde. Le responsable du traitement s'efforcerait raisonnablement d'obtenir un consentement vérifiable, compte tenu des moyens techniques disponibles. Le projet de règlement propose que l'autorité de contrôle sensibilise le public aux risques, aux règles, aux garanties et aux droits relatifs au traitement des données à caractère personnel et que les activités destinées spécifiquement aux enfants (définis comme les personnes de moins de 18 ans) fassent l'objet d'une attention particulière. L'élaboration de codes de conduite spécifiques à l'information et la protection des enfants devrait être encouragée. Il appartiendrait également à la Commission européenne de préciser les règles relatives à la licéité du traitement lorsque des enfants sont concernés.

Le rapporteur souhaite également que soit lancée une campagne d'information destinée à sensibiliser les citoyens, et notamment les plus jeunes, aux enjeux liés à la vie privée et à la protection des données personnelles à l'heure du numérique ainsi qu'à les informer de leurs droits. Il conviendrait aussi de recommander d'imposer un haut niveau de protection par défaut concernant les mineurs ainsi que l'instauration d'obligations et d'exigences spécifiques au traitement des données personnelles des mineurs.

La *mission d'information sur la révolution numérique* a rappelé les enjeux propres à la jeunesse. L'éducation aux médias doit trouver sa place à l'école avec, notamment, un enseignement spécifique d'éducation au numérique. Le renforcement du contrôle parental nécessite d'organiser une campagne d'information et de sensibilisation sur les technologies numériques et leur bon usage par les mineurs. Le rôle des médias dans l'éducation au numérique devrait également être renforcé. Au plan européen, la co-régulation trouve également tout son sens. Une action concertée pour contraindre les réseaux sociaux à appliquer plus strictement l'interdiction de s'inscrire avant un certain âge devrait être menée. Des engagements clairs des fournisseurs d'accès, des hébergeurs et des éditeurs devraient être obtenus en matière d'information destinée à protéger les mineurs.

La Commission européenne propose de renforcer le droit à l'information. La personne serait ainsi informée de la durée pendant laquelle les données seront conservées et de son droit d'introduire une réclamation. La personne devrait être informée lorsque des données sont divulguées pour la première fois à un autre destinataire. Toute personne devrait avoir le droit de se faire communiquer la logique qui sous-tend le traitement des données et les conséquences qu'il pourrait avoir, au moins dans les cas de profilage. Ce droit ne devrait toutefois pas porter atteinte au secret des affaires ou à la propriété intellectuelle.

En matière de profilage, en effet, le nouvel article 20 disposerait que toute personne physique a le droit de ne pas être soumise à une mesure produisant des effets juridiques à son égard ou l'affectant de manière significative qui soit prise sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects personnels ou à analyser ou prévoir le rendement professionnel, la situation économique, la localisation, l'état de santé, les préférences personnelles, la fiabilité ou le comportement.

Le nouvel article 19 propose qu'en matière de marketing direct, le droit de s'opposer au traitement des données soit explicitement proposé à la personne concernée, ce qui est un peu plus précis que le droit actuel.

2. Imposer de nouveaux droits : droit à l'oubli et droit à la portabilité des données

Comme le rappelle le rapport d'information *sur la révolution numérique et les droits de l'individu* précité, les facilités apportées par certaines nouvelles technologies peuvent pousser les individus, par ignorance ou par indifférence, à exposer volontairement des pans entiers de leur vie privée sur Internet. Face à cette nouvelle donne, le droit français et le droit européen, qui prévoient le droit d'accéder à ses données, le droit d'être informé d'un traitement, le droit de s'opposer à figurer dans un fichier pour des motifs légitimes ou, sans justification,

de s'opposer à un traitement à des fins de prospection commerciale, le droit de faire rectifier ou effacer des informations inexactes, ne sont-ils pas dépassés ?

Le droit à l'oubli est régulièrement invoqué et la Commission européenne propose de le consacrer à l'article 17 de la proposition de règlement. Il s'agirait de poser le principe selon laquelle la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données lorsque :

- les données ne sont plus nécessaires pour les finalités prévues ;

- la personne retire son consentement ;

- la personne s'oppose au traitement à des fins de marketing notamment ;

- le traitement n'est pas conforme à la directive.

Le responsable du traitement devrait également avertir les tiers traitant éventuellement lesdites données afin qu'ils les effacent.

La mission d'information a conclu qu'il était nécessaire d'améliorer en amont l'information de l'internaute, en lui offrant des outils lui permettant d'assurer un meilleur contrôle de ses données personnelles. La consécration d'un droit général à l'oubli est apparue peu opérationnelle à la mission d'information. En revanche, il paraissait nécessaire de prévoir, pour les réseaux sociaux, un droit à l'oubli dédié et adapté, qui repose sur :

- un droit exprès et effectif à l'effacement de ses données et non un simple droit de désactivation du profil ;

- la garantie d'une procédure simple et facilement accessible, permettant d'effacer l'intégralité de ses données ou de les récupérer pour 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).

Toutefois, la Commission européenne ayant fait part de son choix d'imposer un droit à l'oubli, il faut soutenir sa démarche ambitieuse et saluer son volontarisme. Il appartient en effet à l'Union européenne et à ses Etats membres de garantir une harmonisation des normes à un niveau élevé de protection des données. Les réseaux sociaux sont bien entendu tout particulièrement visés par une telle disposition. Comme le souligne le rapport sur la révolution numérique[8] :

---

[8] *Page 159.*

« *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. »

En outre, la Commission européenne propose d'instituer en l'article 18 de la proposition de règlement un droit à la portabilité des données, permettant à une personne d'obtenir une copie des données faisant l'objet d'un traitement dans un format électronique couramment utilisé, afin de pouvoir les réutiliser.

B. Du côté des entreprises : entre allégement des charges administratives et exigences de protection accrues

La directive de 1995 prévoit actuellement une obligation générale de notifier les traitements de données aux autorités de contrôle nationales. De l'avis des entreprises et des autorités de contrôle, une telle obligation généralisée n'est ni nécessaire, ni efficace. C'est pourquoi, la Commission européenne propose d'imposer une obligation de notification pour les seuls traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes, du fait de leur nature, de leur portée ou de leurs finalités. Il reviendrait au responsable du traitement de consulter l'autorité de contrôle lorsqu'une analyse d'impact réalisée par le responsable du traitement conclut qu'un traitement présente un degré élevé de risques particuliers ou lorsque les autorités de contrôle nationales ont défini la liste des traitements devant être notifiés préalablement à leur mise en *œuvre*. Cette mesure constituera un allégement significatif des charges des entreprises.

Autre nouveauté, un délégué à la protection des données devrait être systématiquement désigné lorsque le traitement est effectué par une autorité ou un organisme public, lorsque le traitement est effectué par une entreprise de plus de 250 salariés ou lorsque les activités de base du responsable du traitement nécessitent, du fait de leur nature, de leur portée ou de leurs finalités, un suivi régulier et systématique des personnes concernées. Le délégué à la protection des données serait désigné pour une durée minimale de deux ans et son mandat serait reconductible. Il pourrait être un salarié du responsable du traitement ou un prestataire de services. Il aurait une mission d'information et de conseil mais serait

également chargé de contrôler la mise en *œuvre* et l'application des règles internes. Il serait également l'interlocuteur des autorités de contrôle.

Le responsable du traitement devrait, afin de répondre aux nouvelles exigences proposées par le règlement, adopter des règles internes et appliquer des mesures qui répondent aux principes de la protection des données dès la conception (*privacy by design*) et de la protection des données par défaut (article 23) : « *le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées ou conservées au-delà du minimum nécessaire à ces finalités, pour ce qui est tant de la quantité de données que de la durée de leur conservation. En particulier, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques*. »

Les obligations en matière de sécurité des traitements seraient renforcées.

La création de mécanismes de certification, ainsi que de marques et de labels en matière de protection des données devrait être encouragée selon la proposition de règlement. Cette initiative doit également être saluée. Le rapporteur estime que la création de labels permettant d'identifier les logiciels, applications et systèmes offrant des garanties renforcées en matière de protection des données personnelles doit être soutenue. Il faut aussi encourager l'Union européenne à développer 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. Il conviendrait également de soutenir le développement de navigateurs Internet plus protecteurs et plus transparents en matière de ciblage publicitaire.

La question des conséquences négatives des violations des données personnelles serait traitée dans la nouvelle proposition de règlement.

La directive 2009/136/CEE a introduit l'obligation, pour les seuls opérateurs de services de communications électroniques, de notifier à l'abonné ou au particulier la nature d'une violation de données à caractère personnel qui serait intervenue et le contact auprès duquel des informations supplémentaires pourraient être obtenues. Des mesures à prendre pour atténuer les conséquences négatives possibles de la violation des données personnelles devraient être fournies. En parallèle, une notification à l'autorité de contrôle compétente devrait également intervenir.

La proposition de règlement généraliserait cette obligation de notification, à la fois aux autorités de protection des données et aux personnes

concernées, des violations de données personnelles. Il convient de soutenir une telle initiative et de rappeler que les conséquences pour les particuliers concernés peuvent être très lourdes (usurpation d'identité, atteinte à la réputation, vol de coordonnées bancaires, etc.). La notification auprès des personnes ne serait pas obligatoire si le responsable du traitement peut prouver qu'il a mis en place des mesures de protection technologique permettant de rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

C. Préserver les capacités d'action des autorités de protection des données

Le rapporteur juge essentiel que les autorités nationales de protection des données ainsi que le groupe de travail G29 bénéficient de compétences idoines et de ressources suffisantes pour leur permettre de mener à bien leur tâche et garantir leur indépendance. La coopération entre ces autorités devrait être renforcée. A cet égard, la proposition de règlement prévoit la création du comité européen de la protection des données, composé des directeurs des autorités de contrôle nationales et du contrôleur européen de la protection des données. Un mécanisme de contrôle de la cohérence serait établi pour certaines mesures d'application prises par les autorités nationales, afin d'assurer une application homogène du règlement dans les Etats membres.

Un élément de la proposition devrait être combattu, selon lequel le critère de l'établissement principal d'un responsable d'un traitement devrait déterminer quelle autorité nationale de contrôle est compétente pour juger des éventuelles atteintes à la réglementation par ce responsable, quels que soient la nationalité de la personne concernée et son lieu de résidence dans l'Union. La mise en œuvre envisagée au niveau communautaire du critère de l'établissement principal ne pourra susciter qu'une course au « moins-disant » des entreprises. Une seule autorité nationale serait compétente et elle appliquerait en conséquence son droit national à l'ensemble des traitements intervenus dans l'Union. Ceci est nécessairement de nature à favoriser l'implantation des établissements dans les Etats membres réputés les plus accommodants en la matière. Il convient également de rappeler que toutes les autorités de contrôle nationales n'ont pas, loin s'en faut, les capacités d'action, l'expertise et l'expérience que peut avoir la CNIL en France. Une telle disposition ne serait pas acceptable. Par ailleurs, comment expliquer un tel montage aux résidents européens ? Comment pourraient-ils concrètement défendre leurs droits auprès d'autorités de protection des données étrangères, notamment sur des questions aussi complexes ? La Commission européenne prévoit qu'une autorité nationale puisse faire part de son désaccord sur une décision prise par une autre autorité concernant un résident de son territoire.

Le renforcement des possibilités de coercition des autorités nationales, notamment envers les entreprises extra-européennes qui, dans le cadre de leurs activités, ciblent les consommateurs de l'Union, doit être soutenu. Le champ

d'application du droit européen prévu par le nouveau règlement, ainsi que le renforcement des sanctions que les Etats membres pourraient instituer (allant jusqu'à 2 % du chiffre d'affaires mondial de l'entreprise pour les manquements les plus graves), vont, à cet égard, dans la bonne direction.

Enfin, il est regrettable que le projet de règlement prévoit un tel recours à la comitologie : en effet, pour la quasi-totalité des articles, la Commission européenne, assistée d'un comité regroupant les experts des Etats membres, bénéficierait de pouvoirs d'exécution et aurait à définir les actes d'application. Les pouvoirs délégués d'exécution ne doivent en principe pas excéder le champ de questions relativement mineures et techniques. Tel n'est pas le cas ici. Le texte devrait donc être modifié afin de restreindre le recours à la procédure de comitologie.

D. Compléter la proposition de règlement

Il conviendrait de compléter la proposition de règlement sur plusieurs points.

En premier lieu, s'agissant de l'informatique en nuage (« *cloud computing* », des dispositions spécifiques devraient être prévues, ainsi que le recommande la mission d'information sur la révolution numérique dans ses recommandations :

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° 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.

En effet, la gestion des données, qui était jusqu'à présent effectuée par chaque acteur d'Internet pour son compte, peut se faire aujourd'hui différemment, par le transfert des données à un prestataire qui les stocke et les gère à la commande. Cette dissémination des données dans un nuage informatique s'appelle le « *cloud computing* » ou informatique en nuage, car les données circulent en permanence et n'ont plus de localisation propre. Cette pratique permet de réduire les coûts d'exploitation des données et accroît la rapidité ainsi que la souplesse des échanges.

Mais qu'en est-il de la protection de ces données ? Qu'advient-il si le prestataire fait faillite ? Qui est responsable des données et quelle est la loi applicable ? Les serveurs étant mis en réseaux, les données sont-elles localisables ?

Les prestataires qui stockent les données dans des « *data centers* » externalisés permettent de disposer de logiciels performants sans en acheter les licences, d'avoir accès à de nouvelles plateformes de services et de stocker des données en ligne dans des espaces sécurisés. « *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* » (rapport d'information sur la révolution numérique précité, page 202).

Cette problématique est bien entendu très liée à celle du transfert des données vers un Etat tiers. Le transfert de données personnelles peut être légal si :

- la Commission européenne a pris un décision reconnaissant le niveau adéquat de la protection des données dans cet Etat tiers. Seuls quelques pays ont fait l'objet d'une telle décision : Andorre, Argentine, Australie, Canada, Suisse, les Îles Féroé, Guernesey, Israël, l'Île de Man et Jersey. En outre, 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 ;

- la CNIL a vérifié que les clauses contractuelles ou les règles internes de transfert – *binding corporate rules* (dans le cas d'une externalisation à l'intérieur d'un même groupe international) - sont conformes aux dispositions de la loi informatique et libertés. Les clauses contractuelles type ont été précisées par la Commission européenne, conformément à la directive de 1995[9].

[9] *Décision de la Commission européenne 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.*

Par ailleurs, des exceptions permettant tout de même de procéder aux transferts vers des Etats tiers, en dehors de ces règles protectrices, doivent être rappelées : si la personne a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes (sauvegarde de la vie de cette personne, sauvegarde de l'intérêt public, respect d'obligations permettant d'assurer l'exercice d'un droit en justice, consultation d'un registre public qui est destiné à l'information du public, exécution d'un contrat entre le responsable du traitement et l'intéressé, conclusion d'un contrat conclu dans l'intérêt de la personne concernée).

Les clauses contractuelles type élaborées par la Commission européenne n'interdisent pas le transfert de données sensibles, alors que ce type de transfert suscite malgré tout des craintes bien fondées sur les possibilités, pour les personnes intéressées, de faire effectivement valoir leurs droits. En conséquence, la proposition de règlement devrait prévoir un encadrement plus strict s'agissant de l'informatique en nuage.

Enfin, il convient de souligner que le règlement propose de permettre une nouvelle dérogation à l'interdiction de transfert vers un pays tiers dont la Commission n'a pas jugé qu'il assure un niveau de protection adéquat, lorsque le responsable auto-évalue les risques et prend les mesures appropriées (article 44, 1, point h). Cette nouvelle possibilité ne devrait pas être inscrite dans le règlement car elle comprend trop de risques.

En second lieu, le droit au recours des personnes concernées devrait être utilement renforcé par la possibilité de mettre en œuvre des actions de groupe. Comme le souligne le contrôleur européen de la protection des données, dans son avis du 22 juin 2011 sur la communication de la Commission européenne « *une approche globale de la protection des données à caractère personnel dans l'Union européenne* », des mécanismes de recours collectifs pour violation des règles en matière de protection des données devraient être introduits dans la législation de l'Union, dans le but d'habiliter des entités qualifiées à engager des poursuites au nom de groupes de personnes :

« *95. Renforcer les droits des personnes en tant que tels serait inutile, en l'absence de mécanismes procéduraux efficaces pour opposer ces droits. Dans ce contexte, le CEPD recommande l'introduction dans la législation de l'UE de mécanismes de recours collectif en cas de violation des règles en matière de protection des données. Les mécanismes de recours collectif permettant à des groupes de citoyens de combiner leurs différentes plaintes en un seul recours pourraient constituer un outil très efficace pour faciliter l'application de ces règles. Cette innovation est également soutenue par les autorités chargées de la protection des données dans le document des groupes de travail sur l'avenir de la protection de la vie privée*. […]

97. Les recours collectifs sont importants non seulement pour garantir une indemnisation totale ou toute autre mesure de réparation, mais aussi parce qu'ils constituent indirectement un moyen de dissuasion. Le risque de devoir supporter les frais d'une lourde indemnisation collective dans le cadre de telles actions inciterait d'autant plus les responsables du traitement à adopter des mesures efficaces pour s'assurer qu'ils respectent les règles. Sous ce rapport, de meilleures actions de contrôle de l'application des règles par des particuliers au moyen de mécanismes de recours collectif compléteraient les mesures de contrôle des organes publics. »

En troisième lieu, se pose la question de l'anonymisation et de la suppression des données personnelles liées à une adresse IP. Le rapport sur la révolution numérique rappelle :

« *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 rétroingénierie. 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. »

Ces éléments devraient être inscrits dans la règlementation européenne.

CONCLUSION

En conclusion, la proposition de règlement déposée par la Commission européenne, le 25 janvier 2012, consacre de nombreuses avancées essentielles, telles que le droit à la l'oubli, le droit à la portabilité, le renforcement du consentement et de l'information des personnes concernées, l'introduction de concepts tels que celui du respect de la vie privée dès la conception ou du respect de la vie privée par défaut, qui doivent être saluées. Il convient notamment de se féliciter qu'un certain nombre de recommandations formulées dans le cadre de la mission d'information sur la révolution numérique aient pu trouver une traduction dans la proposition de règlement. Il convient à cet égard de rappeler que le rapport de la mission d'information et ses recommandations avaient été adoptés à l'unanimité en commission des lois.

Toutefois, les insuffisances de la proposition doivent également être relevées, qu'il s'agisse notamment de critère de l'établissement principal, de la réglementation applicable à l'informatique en nuage ou encore de la possibilité de mettre en œuvre des actions de groupe.

Enfin, la nécessité d'aller plus loin, au-delà du seul cadre européen, doit être rappelée.

Le rapporteur propose donc l'adoption de la proposition de résolution dont le texte figure en annexe 1.

TRAVAUX DE LA COMMISSION

La Commission s'est réunie le 7 février 2012, sous la présidence de M. Pierre Lequiller, Président, pour examiner le présent rapport.

« **M. Patrick Bloche, rapporteur**. Je souhaite vous présenter la proposition de résolution que j'ai déposée avec mes collègues François Brottes, Jean-Marc Ayrault, Elisabeth Guigou et Jean Grellier. Les évolutions technologiques de la dernière décennie ont créé de nouvelles opportunités d'échanger et d'accéder à l'information.

Ainsi, le développement d'Internet s'est accompagné de l'explosion des réseaux sociaux. Le web est entré dans la vie quotidienne de chacun multipliant ainsi les occasions de faire apparaître ou de transmettre ses données personnelles. La vie privée des personnes – englobant leur réseau d'amis, leurs idées politiques, leur orientation sexuelle ou encore leur religion – est potentiellement visible instantanément par tous et partout via ces sites de socialisation. Pourtant, tous ne sont pas conscients qu'une telle exposition publique de soi risque d'entraîner une perte de contrôle de ses données personnelles.

Par ailleurs, les systèmes de géolocalisation ouvrent un éventail de services tout en possédant un revers qui est de rendre transparents les déplacements de chacun via son téléphone portable, son titre de transport ou de paiement ou encore par l'usage du télépéage. D'autres outils, comme la vidéoprotection ou la biométrie, se sont imposés. Ces technologies partagent un point commun : l'accroissement de la traçabilité des individus et les risques inhérents en matière de respect de la vie privée.

La protection des données personnelles constitue un véritable enjeu juridique et sociétal, mais également économique tant celles-ci sont devenues l'or noir de l'économie numérique. La gratuité des services offerts dans l'environnement en ligne a, de plus en plus souvent, pour contrepartie la collecte, l'usage et le transfert de ces données. Celles-ci font l'objet d'une commercialisation et sont utilisées afin de constituer les profils des utilisateurs-consommateurs, sans aucune information de ces derniers. L'autorégulation ne peut suffire en la matière, c'est pourquoi il convient, par des règles juridiques, de responsabiliser les entreprises.

L'objectif général ne peut être de contrer les changements fondamentaux en cours en matière de service, de communication, d'échange et d'accès à l'information, mais de les accompagner et de les sécuriser. La France, à travers notamment le travail de la CNIL, a imposé un contrôle strict de la captation, du transfert, de l'utilisation et de la conservation des données à

caractère personnel. Selon leur « sensibilité », ces données font l'objet d'une protection plus ou moins forte.

L'adoption, il y a dix-sept ans, de la directive européenne 95/46/CE 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 fut l'acte fondateur de la protection de la vie privée à l'échelle communautaire. Sa modernisation semble désormais à la fois urgente et indispensable. Dans le cadre de sa prochaine révision, le Parlement français se doit de faire valoir un certain nombre de principes, valeurs et droits essentiels.

La protection de la vie privée, et plus globalement de toutes les données personnelles, doit devenir une exigence de fait et de droit au niveau national, mais aussi communautaire et international.

L'analyse que je développe ici est largement alimentée par les travaux de la mission d'information sur la révolution numérique, dont j'étais le rapporteur avec notre collègue Patrice Verchère, conduite en 2011 sous la présidence du Président Jean-Luc Warsmann. L'harmonisation des règles relatives aux données à caractère personnel au niveau de l'Union européenne doit se faire à un niveau élevé de protection.

Il est indispensable de renforcer l'information des personnes dont les données personnelles sont collectées, de s'assurer que celle-ci soit accessible de manière permanente et de permettre à ces personnes un contrôle de leurs données. Il faut, par conséquent, que soit prévue une entière transparence pour les personnes concernées quant au responsable du traitement de leurs données, à leurs destinataires notamment en cas de transfert des données vers des tiers ou vers des applications extérieures, à leur utilisation, à leur durée de conservation, à leur degré de protection ainsi qu'en matière de droit d'accès, de rectification et de suppression de celles-ci. Les propositions de la Commission européenne vont dans le bon sens.

Le consentement en connaissance de cause, préalable et explicite, des personnes dont les données personnelles sont collectées notamment sur le réseau Internet, mais aussi en matière de géolocalisation devrait être prévu.

En ce qui concerne les mineurs, il conviendrait d'imposer un haut niveau de protection par défaut ainsi que l'instauration d'obligations et d'exigences spécifiques au traitement des données personnelles des mineurs.

Toutefois, la réglementation ne suffit pas et une campagne d'information destinée à sensibiliser les citoyens, et notamment les plus jeunes, aux enjeux liés à la vie privée et à la protection des données personnelles à l'heure du numérique ainsi qu'à les informer de leurs droits, devrait être lancée sans attendre.

Il convient de soutenir la reconnaissance d'un « droit à l'oubli » notamment sur les réseaux sociaux qui serait un droit exprès et effectif à l'effacement de ses données, et non un simple droit à la désactivation de son profil, couplé à 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. Il conviendrait également de prévoir 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.

Un certain nombre de propositions de la Commission européenne doivent être soutenues, telles que :

- la création de labels permettant d'identifier les logiciels, applications et systèmes offrant des garanties renforcées en matière de protection des données personnelles ;

- 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 et des particuliers concernés par ces violations ;

- le renforcement des possibilités de coercition des autorités nationales, notamment envers les entreprises extra-européennes qui, dans le cadre de leurs activités, ciblent les consommateurs de l'Union. La règle de compétence proposée dans le règlement ainsi que le renforcement des sanctions vont dans ce sens.

Il convient de compléter la proposition de la commission européenne pour mieux protéger les résidents européens.

En premier lieu, un certain nombre d'évolutions technologiques devraient être mieux encadrées. Il conviendrait d'exclure de « l'informatique en nuage » réalisé hors de l'Union européenne les données personnelles dites « 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. Il conviendrait de faire obligation aux responsables de traitement, et plus particulièrement aux acteurs de « l'informatique en nuage », de réaliser régulièrement des audits de sécurité.

Au-delà de la reconnaissance des principes de protection des données dès la conception et de protection des données par défaut, il convient d'encourager l'Union européenne à développer la recherche, l'innovation et le développement dans le secteur des technologies respectueuses de la vie privée dès leur conception, dites « *privacy by design* ». Il faut en effet 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.

Il faudra également soutenir le développement de navigateurs Internet plus protecteurs et plus transparents en matière de ciblage publicitaire.

L'élaboration d'études d'impact sur la protection des données personnelles de certains produits développés par les entreprises préalablement à leur mise en application devrait être systématisée.

Il conviendrait également de soutenir les recommandations du G29 visant à contraindre les fournisseurs de services, après six mois de conservation, d'une part, à détruire, les références aux adresses IP des utilisateurs de ses services et, d'autre part, à anonymiser complètement ces données.

En second lieu, la place des autorités de contrôle devrait être renforcée.

Il est essentiel que les autorités nationales de protection des données ainsi que le groupe de travail G29 bénéficient de compétences idoines et de ressources suffisantes pour leur permettre de mener à bien leur tâche et garantir leur indépendance. Il convient de renforcer la coopération entre ces autorités.

Le critère de l'établissement principal au niveau communautaire devrait être combattu. Un seul droit national s'appliquerait à une entreprise établie dans plusieurs États membres et, par conséquent, une seule autorité nationale serait compétente. Un tel critère ne pourra susciter qu'une course au « moins-disant » des entreprises vers les Etats membres dans lesquels les autorités de protection sont considérées comme étant les plus souples. Une telle réforme n'est pas acceptable. Il s'agit là d'un point essentiel.

En troisième lieu, s'agissant des possibilités de recours des résidents européens, afin de permettre un droit au recours vraiment effectif, il est nécessaire de rendre possible la mise en œuvre d'actions de groupe en matière de protection des données personnelles.

En quatrième lieu, il faut souligner la nécessité d'un encadrement strict des transferts internationaux des données à caractère personnel et s'opposer au fait que les entreprises puissent, d'elles-mêmes, évaluer la sensibilité de leurs traitements avant un transfert en dehors des cadres de protection européens.

Enfin, devant l'absence d'instrument juridique contraignant au-delà du droit de l'Union et de la convention n° 108 du Conseil de l'Europe, il convient d'appeler à l'adoption par les États membres de l'Union européenne et les États tiers d'une convention internationale pour la protection des personnes à l'égard du traitement des données personnelles, comme le soutient la Résolution de Madrid, adoptée par la 31e Conférence des commissaires à la protection des données et à la vie privée.

En conclusion, la proposition de règlement déposée par la Commission européenne comporte de nombreuses avancées, qui doivent être soutenues. Il fait

néanmoins aller plus loin et, notamment, s'opposer au critère de l'établissement principal. »

L'exposé du rapporteur a été suivi d'un débat, commun à l'examen de ce rapport et de celui de M. Philippe Gosselin sur sa proposition de résolution européenne n° 4227 sur la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

« **Le Président Pierre Lequiller.** Je remercie les rapporteurs pour la qualité de leurs exposés.

M. Guy Geoffroy. Les rapports de nos collègues sont très éclairants. Le chantier sur lequel s'est engagée la Commission européenne constitue un enjeu majeur. Le traitement et la protection des données personnelles sont au cœur de nos préoccupations et j'ai eu souvent à traiter du sujet pour la commission des affaires européennes, notamment sous l'angle du traitement des données des dossiers passagers (PNR).

Ce projet de règlement concerne l'encadrement des traitements de données personnelles qui relevaient auparavant de l'ancien premier pilier. Dans la mesure où il s'agit d'un règlement qui sera d'application directe, il n'y aura pas de transposition, comme c'est le cas lorsqu'une directive est mise en œuvre par les Etats membres. Tout se joue donc maintenant.

C'est pourquoi, je voudrais souligner que si ce texte comporte des avancées bien réelles, certains points sont à combattre avec vigueur.

Ainsi, la possibilité, pour les Etats membres, d'établir leur compétence lorsque les utilisateurs visés sont des résidents européens, même si le lieu d'implantation de l'entreprise est extra-européen est un point très positif. La reconnaissance de nouveaux droits comme le droit à l'oubli et à la portabilité va également dans le bon sens.

Par contre, le critère de l'établissement principal, selon lequel le droit national applicable à tous les traitements de données effectués par une entreprise serait celui de l'Etat membre dans lequel l'établissement principal de l'entreprise est implanté, est inacceptable. Il porte un réel risque de dérive vers le moins-disant, ce qui serait très préjudiciable aux droits des particuliers alors que la Commission européenne fait de la défense des droits des citoyens, une priorité. Ce point doit donc être vivement combattu.

Enfin, il convient de souligner que la réforme présentée par la Commission européenne comprend également un volet relatif à la coopération

policière et judiciaire pénale. La refonte de la décision cadre de 2008 applicable à la protection des données en matière de coopération policière et judiciaire pénale, sur laquelle je serai amené à présenter une communication prochainement, constitue également un enjeu majeur en termes de protection des données. La modification du champ d'application de la décision-cadre, qui ne s'applique qu'aux échanges de données entre Etats membres, et le renforcement des droits des personnes concernées, seront au cœur des négociations.

M^me^ Corinne Erhel. Je voudrais aussi remercier les rapporteurs et excuser François Brottes qui est aussi à l'initiative de la proposition de résolution présentée par M. Patrick Bloche.

On assiste à l'explosion des réseaux sociaux. Derrière cette réussite médiatisée, se trouvent des internautes qui plébiscitent de nombreuses applications qui permettent de publier, sur ces réseaux sociaux, leurs opinions, leurs lectures, leurs déplacements. L'ampleur de ces réseaux est telle qu'ils sont devenus une composante importante de la croissance de nos économies. Leur succès est basé sur leur gratuité, l'audience des sites assurant des revenus publicitaires à leurs éditeurs qui sont de plus en plus en mesure de proposer aux annonceurs des campagnes ciblées grâce aux données dont ils disposent. Les données personnelles peuvent donc être considérées comme l'or noir de l'économie numérique. Face à ce phénomène, il est devenu nécessaire de renforcer l'information et la maîtrise des utilisateurs sur leurs données. Les discours critiques sur Internet et les réseaux sociaux sont nombreux mais ils constituent une véritable révolution culturelle qui a permis aux individus de s'exprimer et de s'informer. Néanmoins, cette possibilité leur est offerte par des fournisseurs de services qui s'approprient des données permettant de les identifier, de les localiser et d'en savoir parfois beaucoup trop sur eux. Ce n'est pas parce que les individus s'exposent plus aisément que nous devons négliger cet aspect fondamental de la protection de l'individu qui est la maîtrise de ses données personnelles. C'est pourquoi le droit à l'oubli sur les réseaux sociaux est un point capital.

L'objectif n'est, ni de pénaliser l'activité des fournisseurs de service, ni de dissuader les utilisateurs d'en faire usage, mais de leur permettre d'user de ces données en toute connaissance de cause et de prévenir des situations contentieuses ou des utilisations malveillantes. Il est nécessaire de fixer des standards élevés de qualité, qui pourront à terme s'imposer comme un élément de différenciation entre les acteurs européens de l'économie numérique. Intégrer la protection des données personnelles dès la conception des services permettrait de distinguer les services respectant ces standards par rapport aux concurrents ne respectant pas de tels critères.

Il faut aussi réserver le stockage des données sensibles aux services de l'informatique en nuages localisés dans l'Union européenne afin d'encourager l'innovation dans ce domaine. La réalisation d'audits de sécurité réguliers est également un point sur lequel nous avons souhaité insister.

Enfin, nous devons considérer spécifiquement le traitement des données relatives aux mineurs, nombreux sur les réseaux sociaux. Ils doivent bénéficier d'une protection renforcée, conformément aux principes de notre droit.

Pour conclure, je rappellerais que les dispositions de la proposition de résolution visent à instaurer une plus grande confiance entre utilisateurs et fournisseurs de service. C'est pourquoi, nous défendons le principe de l'action de groupe et, comme la Commission nationale de l'informatique et des libertés, nous nous opposons à la mise en œuvre, tel que le prévoit le projet, du critère de l'établissement principal afin d'assurer aux citoyens une protection optimale basée sur le principe de proximité.

Le Président Pierre Lequiller. J'aurais souhaité qu'un accord soit possible mais, dans la mesure où cela n'a pas été le cas, je dois mettre aux voix les propositions de résolution.

La proposition de résolution présentée par M. Patrick Bloche est *rejetée*.

M. Philippe Gosselin, rapporteur. Même si nos propositions de résolution sont distinctes, nous essayons d'aller dans le même sens. Il y a bien entendu un vote mais il faut également insister sur nos points communs et je souhaite faire un pas en avant. C'est pourquoi je fais mien le point de la proposition présentée par Patrick Bloche sur l'adoption par les Etats membres de l'Union européenne et les Etats tiers, d'une convention internationale pour la protection des personnes à l'égard du traitement des données personnelles, comme le soutient la Résolution de Madrid, adoptée par la 31ème Conférence des commissaires à la protection des données et de la vie privée. Je propose de l'intégrer par voie d'amendement.

M. Patrick Bloche, rapporteur. Cet amendement est heureux car, en fait, nos deux propositions ne diffèrent réellement que sur la possibilité d'actions de groupe. Dix-sept ans après la mise en œuvre de la directive de 1995, il est essentiel pour la France de peser dans un domaine où elle a été pionnière avec la loi informatique et libertés. Adopter avant la fin de la législature une telle résolution serait un signal très fort. Rappelons enfin que le règlement sera d'application directe et que ce qui se joue aujourd'hui est déterminant. »

La proposition de résolution présentée par M. Philippe Gosselin, ainsi amendée, dont le texte figure ci-dessous, *est adoptée* :

« *L'Assemblée nationale,*

Vu l'article 88-4 de la Constitution,

Vu l'article 151-5 du Règlement de l'Assemblée nationale,

Vu le traité sur le fonctionnement de l'Union européenne, notamment son article 16,

Vu la charte des droits fondamentaux de l'Union européenne, notamment ses articles 7 et 8,

Vu 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,

Vu la loi modifiée n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,

Vu la communication de la Commission européenne au Parlement européen et au Conseil « Une approche globale de la protection des données à caractère personnel dans l'Union européenne » [COM (2010) 609 final],

Vu la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [COM (2012) 11/4/ n° E 7055],

1. Réaffirme son engagement en faveur d'une protection renforcée de la vie privée des citoyens. Cela constitue une exigence démocratique face à l'apparition de nouvelles technologies et à l'émergence d'acteurs mondiaux dont le modèle économique repose notamment sur le traitement commercial de données personnelles ;

2. Soutient les objectifs annoncés par la Commission européenne dans sa communication du 4 novembre 2010 concernant la révision du cadre juridique européen en matière de protection de la vie privée et des données personnelles ;

3. Estime que la modernisation, l'harmonisation et la simplification des règles applicables favoriseront une meilleure prise en compte, par l'ensemble des acteurs, des exigences européennes sur ces questions, grâce notamment à une plus grande responsabilisation des responsables de traitement, qui devront prendre toutes les mesures nécessaires à la protection des données personnelles traitées ;

4. Se félicite à ce titre de l'introduction, au niveau européen, de nouvelles dispositions qui participeront à une meilleure protection des droits des citoyens ;

5. Rappelle les orientations figurant dans la déclaration parlementaire franco-allemande de la mission d'information de l'Assemblée nationale sur les droits de l'individu dans la révolution numérique et de la commission d'enquête du Bundestag sur Internet et la société numérique, en date du 19 janvier 2011 ;

6. Souligne ainsi l'inscription dans le texte proposé par la Commission européenne d'un droit à l'oubli pour les citoyens qui devrait, dans un souci de réalisme, être applicable aux réseaux sociaux et qui permettra aux personnes d'obtenir plus simplement la suppression de leurs données personnelles par les responsables de traitement. Il conviendra toutefois de s'assurer que ce droit permette aux personnes concernées d'obtenir la suppression des données mises en ligne par un tiers ;

7. Se prononce également en faveur de l'introduction d'un nouveau droit à la portabilité des données personnelles pour les citoyens qui pourront désormais obtenir, à leur demande, restitution des données traitées, et notamment pour celles publiées sur les réseaux sociaux, dans un format électronique qui permette leur réutilisation sur d'autres supports ;

8. Défend la proposition de la Commission européenne visant à modifier considérablement les règles de recueil du consentement des citoyens au traitement de leurs données personnelles. Cette disposition sera beaucoup plus protectrice puisque l'expression du consentement nécessitera désormais une action positive du citoyen. Son silence ou son inaction ne pourront plus être assimilés à un consentement implicite ;

9. Soutient la désignation de délégués à la protection des données au sein des administrations publiques et des entreprises de plus de 250 salariés. Cette disposition, particulièrement attendue par certaines autorités de protection européennes, participera assurément à une meilleure prise en compte des règles applicables dans ce domaine et à une plus grande sensibilisation des structures publiques et privées à ces questions. Toutefois, le caractère obligatoire de la désignation pourrait être contre-productif, une attention particulière devant être portée à la situation des salariés désignés délégués à la protection des données ;

10. Exprime son opposition claire à l'inscription, dans le texte proposé par la Commission européenne, du critère du principal établissement du responsable de traitement, qui serait porteur de conséquences politiques et économiques extrêmement dommageables pour notre pays, et pour l'ensemble du territoire européen ;

11. Considère que cette solution éloignerait les Européens des autorités compétentes et qu'elle irait à l'encontre de la construction d'une Europe politique et concrète, proche des préoccupations de ses citoyens. Elle favoriserait également la pratique du « forum shopping », et l'établissement d'entreprises au sein des Etats membres dont les autorités de protection privilégient une approche plus souple. Elle réduirait également considérablement l'attractivité des territoires français et européens ;

12. Défend une solution alternative, fondée sur le maintien de la compétence d'une autorité de protection d'un Etat sur tout traitement de données

ciblant spécifiquement la population de cet Etat, quel que soit l'Etat membre sur lequel est établi le responsable de traitement ;

13. Exprime ses plus vives inquiétudes quant au mécanisme de coopération proposé par la Commission européenne, qui ne garantirait pas une information suffisante des autorités de protection, notamment dans les cas de traitement de données particulièrement sensibles, comme les données génétiques, biométriques, ou les données de santé, réduisant considérablement les contrôles a priori sur ces traitements à risques. Elle soutient l'introduction de nouvelles dispositions permettant une coopération renforcée entre les autorités de protection, afin notamment de garantir un contrôle rigoureux des traitements de données à risques ;

14. Regrette la concentration de pouvoirs considérables entre les mains de la Commission européenne, aux dépends des autorités de protection, quant à l'élaboration des lignes directrices en matière de protection des données personnelles et à la définition des modalités d'application des nouvelles dispositions. Elle défend un rééquilibrage de ces compétences au profit des autorités de protection qui bénéficient de l'expertise technique indispensable à cette mission ;

15. Appelle à un meilleur encadrement des transferts internationaux de données, qui doivent nécessairement préserver les pouvoirs de contrôle et d'autorisation de ces échanges des autorités nationales de protection. L'auto-évaluation des conditions de transferts, par les responsables de traitement eux-mêmes, conduirait à une baisse considérable du niveau de protection des droits des citoyens ;

16. Invite le Gouvernement français à se saisir de cette question dans les plus brefs délais et à défendre une réforme plus respectueuse des droits de nos concitoyens, en accord avec la position défendue publiquement par la Commission nationale de l'informatique et des libertés ;

17. Appelle à l'adoption, par les États membres de l'Union européenne et les États tiers, d'une convention internationale pour la protection des personnes à l'égard du traitement des données personnelles, comme le soutient la résolution de Madrid, adoptée par la 31e conférence internationale des commissaires à la protection des données et de la vie privée. »

La Commission *a approuvé* la proposition de règlement (E 7055) sous réserve des observations formulées dans la proposition de résolution.

ANNEXE 1 :
PROPOSITION DE RESOLUTION
(rejetée par la Commission des affaires européennes)

PROPOSITION DE RESOLUTION EUROPEENNE RELATIVE A LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL AU SEIN DE L'UNION EUROPEENNE, NOTAMMENT DANS LE CADRE DE LA REFORME DE LA DIRECTIVE 95/46/CE,

Article unique

L'Assemblée nationale,

Vu l'article 151-5 du Règlement de l'Assemblée nationale,

Vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

Vu la charte des droits fondamentaux de l'Union européenne, notamment ses articles 7 et 8,

Vu la convention européenne de sauvegarde des Droits de l'Homme et des libertés fondamentales (CEDH), notamment son article 8 relatif a la protection de la vie privée et familiale,

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative a la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques »),

Vu les conclusions du Conseil relatives à la communication de la Commission intitulée « Une approche globale de la protection des données à caractère personnel dans l'Union européenne »,

Vu le rapport du Parlement européen sur une approche globale de la protection des données à caractère personnel dans l'Union européenne, 22 juin 2011,

Vu l'avis du contrôleur européen de la protection des données (CEPD) du 14 janvier 2011 sur la communication de la Commission intitulée « Une approche globale de la protection des données à caractère personnel dans l'Union européenne »,

Vu la contribution du groupe de travail « Article 29 » sur la protection des données à la consultation de la Commission sur le cadre juridique du droit fondamental à la protection des données à caractère personnel intitulée « L'avenir de la protection de la vie privée »,

Vu la « Résolution de Madrid » pour l'établissement de normes internationales sur la vie privée et la protection des données personnelles, adoptée le 5 novembre 2009 par la 31e Conférence des commissaires à la protection des données et à la vie privée,

Vu l'article 1er de la loi française « informatique et libertés » du 6 janvier 1978 qui dispose que « 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 privée, ni aux libertés individuelles ou publiques »,

Vu le rapport d'information sur les droits de l'individu dans la révolution numérique présenté par MM. Patrick Bloche et Patrice Verchère, Assemblée nationale, no 3560, 22 juin 2011,

Vu le rapport d'information de M. Yves Détraigne et Mme Anne-Marie Escoffier, « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », fait au nom de la commission des lois du Sénat, no 441, 27 mai 2009,

Considérant que constitue une donnée à caractère personnel, en vertu de l'article 2 de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ; pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ;

Considérant que les évolutions technologiques permettent une intensification et une rapidité croissante des transferts de données à caractère personnel ;

Considérant que de nombreux acteurs économiques transfrontaliers tels que les réseaux sociaux ont pour objet de leur activité la mise à disposition et le partage de données à caractère personnel ;

Considérant que les systèmes de traitement de données à caractère personnel doivent être au service des citoyens et doivent ainsi respecter les libertés et droits fondamentaux des personnes dont leur vie privée ;

Considérant que l'article 8 de la Charte des droits fondamentaux de l'Union européenne détermine que « toute personne a droit à la protection des données à caractère personnel la concernant », que « 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 » et que « le respect de ces règles est soumis au contrôle d'une autorité indépendante » ;

Considérant que les mineurs doivent bénéficier d'une protection particulière ;

Considérant que l'harmonisation du droit au niveau communautaire doit avoir pour objectif une protection juste et efficace des données à caractère personnel et non un alignement sur le « moins disant » ;

1. Appelle à l'adoption par les États membres de l'Union européenne et les États tiers d'une convention internationale pour la protection des personnes à l'égard du traitement des données personnelles, comme le soutient la Résolution de Madrid, adoptée par la 31e Conférence des commissaires à la protection des données et à la vie privée ;

2. Considère que l'harmonisation des règles relatives aux données à caractère personnel au niveau de l'Union européenne doit se faire à un niveau élevé de protection ;

3. Souhaite que soit lancée une campagne d'information destinée à sensibiliser les citoyens, et notamment les plus jeunes, aux enjeux liés à la vie privée et à la protection des données personnelles à l'heure du numérique ainsi qu'à les informer de leurs droits ;

4. Juge indispensable de renforcer l'information des personnes dont les données personnelles sont collectées, de s'assurer que celle-ci soit accessible de manière permanente et de permettre à ces personnes un contrôle de leurs données ; souhaite, par conséquent, que soit prévue une entière transparence pour les personnes concernées quant au responsable du traitement de leurs données, leurs destinataires notamment en cas de transfert des données vers des tiers ou vers des applications extérieures, leur utilisation, leur durée de conservation, leur degré de

protection ainsi qu'en matière de droit d'accès, de rectification et de suppression de celles-ci ;

5. Estime nécessaire que soit prévu le consentement en connaissance de cause, préalable et explicite, des personnes dont les données personnelles sont collectées notamment sur le réseau internet mais aussi en matière de géolocalisation ;

6. Propose la reconnaissance d'un « droit à l'oubli » notamment sur les réseaux sociaux qui serait un droit exprès et effectif à l'effacement de ses données et non un simple droit à la désactivation de son profil couplé à 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 ; de plus, suggère 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 ;

7. Recommande d'imposer un haut niveau de protection par défaut concernant les mineurs ainsi que l'instauration d'obligations et d'exigences spécifiques au traitement des données personnelles des mineurs ;

8. Considère qu'il convient d'exclure de « l'informatique en nuage » réalisé hors de l'Union européenne les données personnelles dites « 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 ;

9. Souligne la nécessité d'un encadrement strict des transferts internationaux des données à caractère personnel ;

10. Encourage l'Union européenne à développer 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 ;

11. Soutient le développement de navigateurs Internet plus protecteurs et plus transparents en matière de ciblage publicitaire ;

12. Propose la création de labels permettant d'identifier les logiciels, applications et systèmes offrant des garanties renforcées en matière de protection des données personnelles ;

13. Recommande l'élaboration d'étude d'impact sur la protection des données personnelles de certains produits développés par les entreprises préalablement à leur mise en application ;

14. Est favorable au fait de faire obligation aux responsables de traitement, et plus particulièrement les acteurs de « l'informatique en nuage », de réaliser régulièrement des audits de sécurité ;

15. Souhaite obliger tout responsable de traitements de données à caractère personnel à notifier les failles de sécurité auprès de l'autorité nationale de protection des données personnelles et des particuliers concernés par ces violations ;

16. Soutient les recommandations du G29 visant à contraindre les fournisseurs de services, après six mois de conservation, d'une part, à détruire, les références aux adresses IP des utilisateurs de ses services et, d'autre part, à anonymiser complètement ces données ;

17. Souhaite rendre possible la mise en œuvre d'action de groupe en matière de protection des données personnelles ;

18. Juge essentiel que les autorités nationales de protection des données ainsi que le groupe de travail G29 bénéficient de compétences idoines et de ressources suffisantes pour leur permettre de mener à bien leur tâche et garantir leur indépendance ; invite, par ailleurs, à renforcer la coopération entre ces autorités ;

19. Se prononce pour le renforcement des possibilités de coercition des autorités nationales, notamment envers les entreprises extra-européennes qui, dans le cadre de leurs activités, ciblent les consommateurs de l'Union ;

20. S'oppose à la mise en œuvre envisagée au niveau communautaire du critère de l'établissement principal qui ne pourra susciter qu'une course au « moins-disant » des entreprises (ainsi, dans l'hypothèse d'une directive européenne, un seul droit national s'appliquerait à une entreprise établie dans plusieurs États membres et, en cas de règlement européen, une seule autorité nationale serait compétente).

ANNEXE 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.

ANNEXE 3 :
MISSION D'INFORMATION « RÉVOLUTION NUMÉRIQUE ET DROITS DE L'INDIVIDU : POUR UN CITOYEN LIBRE ET INFORMÉ »

SYNTHESE 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.