XIVe LÉGISLATURE

COMMISSION DE RÉFLEXION ET DE PROPOSITIONS SUR LE DROIT ET LES LIBERTÉS À L'ÂGE DU NUMÉRIQUE

NUMÉRIQUE ET LIBERTÉS :

Un nouvel âge démocratique

Rapport n° 3119

Présenté par
M. Christian PAUL
et Mme Christiane FÉRAL-SCHUHL
Co-Présidents

ASSEMBLÉE NATIONALE

Composition de la Commission

Co-présidents :

M. Christian Paul, député de la Nièvre, Groupe Socialiste, républicain et citoyen ;

Mme Christiane Féral-Schuhl, ancien bâtonnier de l'Ordre des avocats du barreau de Paris (2012-2014), avocate au barreau de Paris depuis 1981 spécialisée en droit de l'informatique et des nouvelles technologies, cofondatrice du cabinet Féral-Schuhl-Sainte-Marie, ancienne présidente du conseil d'administration de l'Association de droit de l'informatique juridique (2000-2010) ;

Députés :

M. Patrick Bloche, député de Paris, Groupe Socialiste, républicain et citoyen ;

M. Sergio Coronado, député des Français établis hors de France, Groupe Écologiste ;

M. Charles de Courson, député de la Marne, Groupe Union des démocrates et indépendants ;

Mme Virginie Duby-Muller, députée de Haute-Savoie, Groupe Les Républicains ;

Mme Laurence Dumont, députée du Calvados, Groupe Socialiste, républicain et citoyen ;

Mme Corinne Erhel, députée des Côtes-d'Armor, Groupe Socialiste, républicain et citoyen ;

Mme Gilda Hobert, députée du Rhône, Groupe Radical, républicain, démocrate et progressiste ;

Mme Laure de La Raudière, députée de l'Eure-et-Loir, Groupe Les Républicains ;

Mme Martine Martinel, députée de Haute-Garonne, Groupe Socialiste, républicain et citoyen ;

M. Franck Riester, député de Seine-et-Marne, Groupe Les Républicains ;

M. Gabriel Serville, député de Guyane, Groupe Gauche démocrate et républicaine ;

M. Patrice Verchère, député du Rhône, Groupe Les Républicains ;

Personnalités qualifiées :

M. Philippe Aigrain, informaticien et chercheur, ancien directeur du secteur technique du logiciel à la Commission européenne (1996-2003), fondateur et président-directeur-général de Sopinspace, qui développe notamment des logiciels libres, co-fondateur de La Quadrature du net ;

M. Godefroy Beauvallet, ingénieur en chef des télécommunications, directeur du fonds AXA pour la recherche, membre du Conseil national du numérique, maître de conférence associé à Télécom ParisTech ;

Mme Valérie-Laure Benabou, professeur des universités, professeur agrégé de droit privé à l'Université de Versailles Saint-Quentin-en-Yvelines, personnalité qualifiée au Conseil supérieur de la propriété littéraire et artistique ;

M. Jean Dionis du Séjour, maire d'Agen, ancien député, rapporteur au nom de la commission des affaires économiques de la loi pour la confiance dans l'économie numérique en 2003-2004 ;

M. Daniel Le Métayer, directeur de recherche à l'INRIA, établissement public de recherche dédié aux sciences du numérique, au centre de recherche Grenoble – Rhône-Alpes à Lyon responsable de l'INRIA Project Lab CAPPRIS (Collaborative Action on the Protection of Privacy Rights in the Information Society) ;

M. Winston Maxwell, avocat associé du cabinet Hogan Lovells, spécialiste des droits français et européen des communications, du droit des médias et de la neutralité du net, co-président du comité sur l'économie numérique de la chambre de commerce franco-américaine ;

Mme Francesca Musiani, sociologue, chercheuse à MINES ParisTech, docteur en socio-économie de l'innovation (Thèse intitulée « Nains sans géants. Architecture décentralisée et services Internet », lauréate du prix de thèse « Informatique et Libertés » de la CNIL en 2014) ;

M. Edwy Plenel, journaliste, président et directeur de la publication du site d'information en ligne Mediapart, ancien directeur de la rédaction du Monde, secrétaire général du Syndicat de la presse indépendante d'information en ligne (SPIIL) ;

Mme Myriam Quémener, magistrate au parquet général de la cour d'appel de Versailles, précédemment sous-directrice de la justice pénale générale à la direction des affaires criminelles et des grâces au ministère de la Justice (2004-2007), substitute du procureur général près la cour d'appel de Versailles (2007-2012), procureur de la République adjoint près le tribunal de grande instance de Créteil (2012-2013) ;

Mme Thaima Samman, avocate, membre des barreaux de Paris et Bruxelles, anciennement directrice du département juridique et affaires publiques à Microsoft France puis Associate General Counsel, Senior Director Corporate Affairs/CSR à Microsoft Europe, Moyen-Orient et Afrique ;

M. Henri Verdier, directeur de la mission Etalab au secrétariat général pour la modernisation de l'action publique, entrepreneur numérique (associé et co-fondateur de la société MFG-R&D), personnalité qualifiée au sein du comité de prospective de l'ARCEP ;

M. Cyril Zimmermann, fondateur et président-directeur-général de Hi-Media, entreprise française spécialisée dans la monétisation de l'audience, et de Hi-Cab, société de moto-taxi, président de l'Acsel, l'association de l'économie numérique.

SOMMAIRE

—

Pages

INTRODUCTION 9

I. RENFORCER LE DROIT À L'INFORMATION À L'ÈRE NUMÉRIQUE 21

A. CONSACRER UN DROIT FONDAMENTAL À L'INFORMATION D'INTÉRÊT PUBLIC 22

1. Un droit d'accès aux documents administratifs ancien mais conditionné et inabouti 22

a. Un droit d'accès individuel et « à la demande » conditionné 23

b. Un droit d'accès inabouti 24

2. L'absence d'offre globale et satisfaisante d'informations publiques 26

a. Une diffusion croissante mais partielle des informations publiques 26

b. Un mouvement d'ouverture des données publiques dynamique mais encore à ses débuts 27

3. Instaurer un véritable « droit de savoir » à l'égard de l'ensemble des informations intéressant la vie publique et démocratique 31

a. La nécessité d'instaurer un droit à l'information d'intérêt public 31

b. Élargir la liste des documents communicables à l'ensemble des informations intéressant la vie publique et démocratique 35

B. ORGANISER LE DROIT À L'INFORMATION PUBLIQUE À L'ÈRE NUMÉRIQUE 43

1. Généraliser la mise en ligne des informations publiques, sauf lorsqu'elle est manifestement impossible ou trop coûteuse 44

2. Inscrire dans la loi le principe d'ouverture des données publiques à des fins de libre et gratuite réutilisation 45

a. Poser dans la loi le principe d'ouverture des données publiques 45

b. Inscrire dans la loi le principe de réutilisation libre et gratuite des données publiques 48

C. RENFORCER LA PROTECTION DES LANCEURS D'ALERTE 51

1. Un cadre juridique segmenté et partiel 52

a. Des mécanismes de signalement et de protection de leurs auteurs… 53

b. … mais aucun dispositif général de protection des lanceurs d'alerte 54

2. Créer un statut général protecteur des « lanceurs d'alerte » 56

a. Élargir le champ du « droit d'alerte » aux faits manifestement contraires à l'intérêt général..... 57

b. Garantir une protection effective aux « lanceurs d'alerte » 58

II. DÉFENDRE LA LIBERTÉ D'EXPRESSION À L'ÈRE NUMÉRIQUE..... 61

A. AFFIRMER LE PRINCIPE DE NEUTRALITÉ TECHNOLOGIQUE 63

1. L'application de plein droit à internet de la loi du 29 juillet 1881..... 63

2. L'exclusion de plein droit d'internet du régime de l'audiovisuel 64

3. La nécessité de justifier tout traitement différencié fondé sur la technologie..... 67

B. PRÉSERVER LA LOI DU 29 JUILLET 1881 SUR LA PRESSE, PILIER DE LA DÉMOCRATIE, AUJOURD'HUI MENACÉE 70

1. L'exclusion de l'apologie du terrorisme et de la provocation au terrorisme hors de la loi sur la presse : un effet de brèche majeur 71

2. L'annonce d'un projet visant à basculer de nouveaux délits d'opinion hors de la loi sur la presse : vers la fin de la loi sur la presse ? 73

3. Se garder d'une conception de la liberté d'expression à deux vitesses..... 75

C. CONFORTER LA PLACE DU JUGE COMME GARANT DE LA LIBERTÉ D'EXPRESSION..... 76

1. Limiter le rôle de « censeurs » des intermédiaires privés 77

a. Les incertitudes sur la ligne de démarcation entre hébergeur et éditeur et l'objectif de « régulation des plateformes » n'appellent pas la création d'une nouvelle catégorie dans la LCEN 80

b. Le critère du « manifestement illicite » : un rempart insuffisant contre la censure privée..... 84

c. Réaffirmer les obligations limitées des hébergeurs dans la lutte contre les contenus illégaux 86

2. Limiter les cas de contournement du juge par les autorités administratives..... 89

a. N'autoriser le blocage qu'à titre subsidiaire et sur décision judiciaire 90

b. Limiter les cas de contournement du juge par les autorités administratives 93

3. Renforcer les moyens d'action contre les contenus illégaux dans le respect du rôle du juge..... 96

a. Renforcer en profondeur les moyens d'action de la justice 96

b. Renforcer l'accessibilité et l'effectivité de la loi de 1881..... 98

c. Garantir les conditions d'une meilleure coopération des hébergeurs 99

d. Renforcer les dispositifs de signalement sur les plateformes..... 100

III. REPENSER LA PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES À CARACTÈRE PERSONNEL 103

A. RÉÉVALUER L'IMPORTANCE DES DROITS AU RESPECT DE LA VIE PRIVÉE ET À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL 107

1. Faire des droits au respect de la vie privée et à la protection des données personnelles des droits fondamentaux constitutionnellement garantis 107

a. La massification de la collecte et la diversification des usages des données à caractère personnel 108

b. Des normes constitutionnelles paradoxalement silencieuses 109

c. Vers une constitutionnalisation des droits au respect de la vie privée et à la protection des données à caractère personnel ? 111

2. Retenir une conception extensive des informations personnelles protégées par ce droit 113

a. La modification de la nature des données personnelles traitées à l'ère numérique 113

b. La protection actuelle des données identifiantes 115

c. Retenir une interprétation large de la notion de donnée à caractère personnel 116

d. Renforcer l'efficacité des techniques d'anonymisation des données personnelles 117

3. Recourir à de nouveaux instruments de protection de la vie privée et des données 118

a. Encourager le recours aux technologies protectrices de la vie privée et des données personnelles 118

b. Repenser la régulation des responsables de traitements 122

c. Mettre en place une protection harmonisée des citoyens au niveau européen 128

B. DONNER À L'INDIVIDU L'AUTONOMIE INFORMATIONNELLE ET DÉCISIONNELLE NÉCESSAIRE À SON LIBRE ÉPANOUISSEMENT DANS L'UNIVERS NUMÉRIQUE 131

1. Privilégier le droit à l'autodétermination de l'individu dans l'usage de ses données personnelles 131

a. Écarter la contractualisation du droit au respect de la vie privée 131

b. Consacrer un droit à l'autodétermination informationnelle des individus à l'ère numérique 133

2. Conserver le principe du consentement préalable de l'individu en l'adaptant au contexte de collecte de ses données 136

a. Le consentement préalable est l'une des conditions de licéité d'un traitement 136

b. Les limites du consentement à l'ère numérique 137

c. Conserver le principe du consentement préalable en adaptant sa portée normative et les modalités de son recueil au contexte de la collecte et du traitement des données 139

3. Reconnaître à l'individu de nouveaux droits au service de son libre arbitre et de son libre agir 141

a. Renforcer l'effectivité des droits reconnus à l'individu 142

b. Accroître les droits des individus face aux algorithmes 147

c. Doter les individus des moyens juridiques de faire cesser un manquement à la législation en matière de protection des données personnelles 148

C. CONFORTER LA PROTECTION DE LA SPHÈRE PRIVÉE À L'HEURE DE LA SURVEILLANCE INSTITUTIONNELLE 151

1. Des règles inadaptées à la protection des droits fondamentaux à l'ère numérique 152

a. La faiblesse du cadre juridique applicable aux activités de renseignement 152

b. La redéfinition des prérogatives des services de police judiciaire et administrative 156

2. Définir un régime juridique global, cohérent et protecteur des libertés fondamentales pour les activités de renseignement 159

3. Mieux encadrer les nouveaux moyens donnés par le numérique aux services de police et de justice 167

IV. DÉFINIR DE NOUVELLES GARANTIES INDISPENSABLES À L'EXERCICE DES LIBERTÉS À L'ÈRE NUMÉRIQUE 171

A. LE DROIT D'ACCÈS À INTERNET : UN DROIT À RENFORCER 171

1. Le droit d'accès à internet, une reconnaissance dont la portée demeure limitée 172

2. Un droit à renforcer 175

B. LA NEUTRALITÉ DES RÉSEAUX : UN PRINCIPE À CONSACRER 177

1. Un principe fondateur d'internet, aujourd'hui menacé par les pratiques des opérateurs 178

a. Un principe fondateur d'internet 178

b. Un principe menacé par l'évolution des pratiques des opérateurs 179

2. Un principe qui doit être plus clairement consacré dans le droit positif 180

a. De premiers éléments de reconnaissance dans le droit positif 180

b. Les débats sur la définition du principe à consacrer au plan européen 187

c. Consacrer clairement le principe de neutralité du net dans une définition exigeante 192

C. LA « LOYAUTÉ DES PLATEFORMES » : UN OBJECTIF À ATTEINDRE PAR L'ADAPTATION DU DROIT COMMUN ET LA MISE EN PLACE D'UNE RÉGULATION SPÉCIFIQUE DES GRANDES PLATEFORMES 196

1. De la neutralité à la loyauté des plateformes 197

a. Une volonté initiale d'extension du champ de la neutralité d'internet 197

b. De la neutralité à la loyauté 198

2. La « loyauté des plateformes » : une notion à clarifier sans retard 199
a. Les plateformes numériques : une nouvelle catégorie d'acteurs qui présente des caractéristiques et problématiques spécifiques 199
b. La « loyauté des plateformes » : une notion majeure, à mieux appréhender juridiquement 202
i. La loyauté des plateformes selon le Conseil d'État 203
ii. La loyauté des plateformes selon le Conseil national du numérique 205
3. Deux grandes approches possibles pour appréhender les plateformes 207
a. Une approche par l'adaptation du droit commun 208
i. Le droit de la concurrence 209
ii. Le droit commercial 214
iii. Le droit de la consommation 216
iv. Le droit de la protection des données à caractère personnel 217
v. Le droit fiscal 217
b. Une approche par la mise en place d'une régulation spécifique 218
i. De nombreux acteurs et observateurs appellent à la mise en place d'une régulation spécifique de ces acteurs. 218
ii. Les difficultés posées par la mise en place d'une telle régulation ne doivent pas être sous-estimées, à commencer par la définition de son champ. 219
V. DESSINER UNE NOUVELLE FRONTIÈRE ENTRE PROPRIÉTÉ ET COMMUNS 227
A. LE DÉVELOPPEMENT DES COMMUNS NUMÉRIQUES 229
B. RENFORCER LA PLACE DES COMMUNS DANS LA SOCIÉTÉ NUMÉRIQUE 232
1. Donner un statut de droit positif aux communs et au domaine public 232
2. La conciliation des droits ou capacités d'usage et des droits de propriété intellectuelle 238
a. Sur l'application du droit d'auteur à la sphère non marchande 239
b. Sur la possibilité de reconnaître des droits culturels 240
3. Renforcer les droits des créateurs au titre de l'exploitation numérique de leurs œuvres et favoriser des modèles de rémunération équitable 244
4. Approfondir le droit à l'exploitation et au partage des connaissances scientifiques : le libre accès (*open access*) 246
SOMMAIRE DES ANNEXES 251

INTRODUCTION

MESDAMES, MESSIEURS,

Toute révolution industrielle appelle un nouvel âge démocratique. Telle est la conviction qui a animé les travaux de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, composée à parité de député-e-s de l'Assemblée nationale et de représentant-e-s de la société civile.

Bouleversant notre relation au temps – désormais immédiat – et à l'espace – devenu sans frontières –, l'actuelle révolution technologique est à l'origine d'un ébranlement général de nos sociétés, dans leurs pratiques culturelles et leurs modes de consommation, la sphère économique et le monde du travail, les accès aux savoirs et la liberté d'expression, l'espace public comme la sphère de l'intimité... Or, **la direction que prendra ce mouvement inédit n'est pas définie par avance** : l'effet final des techniques, qui peuvent être aussi bien libératrices qu'asservissantes, dépend toujours des usages sociaux qui s'imposeront à la longue.

C'est ici que se pose **la question décisive de la réponse collective qu'inventeront nos sociétés devant cette accélération** qui les affole et les fascine, les réjouit autant qu'elle les inquiète, entre découverte d'un futur inédit et perte de repères anciens. Car ces temps planétaires de révolution objective, concrète et matérielle, où de vieux mondes se meurent tandis que les nouveaux sont encore incertains, cherchent à tâtons leur issue politique dans une histoire qu'il nous revient d'écrire, entre chute dans la barbarie et sursaut dans la démocratie.

Les deux précédentes révolutions industrielles de notre modernité, dont les moteurs technologiques étaient la machine à vapeur pour la première et l'électricité pour la deuxième, ont dû faire face au même défi, non sans régressions, détours et dégâts, voire catastrophes, qui sont autant d'alertes pour notre présent. Faute d'invention démocratique nouvelle, rénovant la promesse initiale de liberté, d'égalité et de fraternité, **des fuites en avant autoritaires et inégalitaires peuvent s'imposer comme réponses aux doutes et incertitudes** suscités par l'émergence de ce nouveau monde, ses destructions créatrices, ses bouleversements géopolitiques, ses ébranlements culturels.

La priorité de l'heure, et pour laquelle nous avons déjà trop tardé à nous mobiliser, est donc celle **du nouvel écosystème démocratique nécessaire** afin d'éviter que la révolution numérique ne soit soumise à la loi du plus fort ou du plus bruyant, du plus sauvage ou du plus violent, du plus marchand ou du plus autoritaire. Afin, en somme, qu'elle favorise une renaissance de l'idéal démocratique, par l'approfondissement de ses méthodes et l'élargissement de ses publics.

Hier énoncé comme une promesse de principe, un droit universel devient soudain réalité tangible. Formulé par l'article 19 de la Déclaration universelle des droits de l'homme du 10 décembre 1948, le droit de tout individu *« de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit »* est désormais devenu une potentialité ouverte à n'importe qui, n'importe où et n'importe comment, sur des supports divers et sous des formats multiples.

Devant cette évidente bonne nouvelle, l'enjeu d'une délibération collective est d'énoncer les conditions pour que cette liberté ne se retourne pas contre elle-même. De faire en sorte qu'elle ne soit pas confisquée ou détournée, trahie ou corrompue. Telle est l'ambition des propositions issues des travaux de cette Commission : dans la diversité de leurs sensibilités, partisanes ou professionnelles, ses membres font le choix de **parier sur l'énergie démocratique que peut libérer la révolution numérique, alors même que nos sociétés doutent d'elles-mêmes.**

De ce point de vue, leurs réflexions rejoignent l'esprit qui, lors de la précédente révolution industrielle, celle de l'avènement progressif d'une information de masse, présida aux patients travaux parlementaires qui, en 1881, donnèrent naissance à cette formidable avancée démocratique que fut la loi sur la liberté de la presse. Il fallait alors bien des audaces pour mettre fin à une accumulation contraignante de quarante-deux lois, tenant pour la plupart en méfiance la liberté de dire et le droit de savoir, afin de les remplacer par cet énoncé aussi simple qu'émancipateur, celui de l'article 1er : *«* [l]*'imprimerie et la librairie sont libres »*. Or ce pari radical sur la liberté ne fut pas sans incidence sur la créativité législative et l'inventivité politique de la Troisième République, enfin installée à demeure, durant ses trois premières décennies, jusqu'en 1914.

Aujourd'hui encore, plutôt que de craindre une liberté nouvelle, ses audaces ou ses excès, il s'agit donc d'en faciliter, d'en protéger et d'en qualifier l'exercice. Car ce sera la meilleure protection de la démocratie elle-même, par la construction d'un espace public délibératif et participatif qui la consolide et la fortifie. Dans *Le Bon Gouvernement* (1), M. Pierre Rosanvallon souligne combien ce dernier repose sur un impératif de « *lisibilité* », de façon à ce que l'action des gouvernants soit intelligible par les gouvernés afin qu'en retour, ceux-ci puissent

(1) Seuil, 2015.

être des citoyens actifs, investis parce qu'informés, impliqués parce que concernés.

C'est cette exigence démocratique qu'entend promouvoir ce rapport. Il y répond en proposant de consacrer, d'organiser et de renforcer un droit fondamental à l'information d'intérêt public ; de défendre la liberté d'expression dans l'espace public en affirmant le principe de neutralité technologique et en confortant une justice indépendante comme son seul garant ; de consolider son indispensable corollaire, la protection de la sphère privée, en responsabilisant chaque individu comme le premier acteur de sa liberté ; d'approfondir le droit d'accès à internet, par la neutralité des réseaux et la loyauté des plateformes ; d'ouvrir la perspective des « communs », où se construit un espace ni marchand ni étatique de partage et d'échange.

Il s'agit rien de moins, pour nos concitoyens, que de « *retrouver un rapport positif à l'avenir* », pour suivre de nouveau M. Pierre Rosanvallon : l'avenir « *comme possibilité d'une maîtrise du monde, comme capacité de faire consciemment l'histoire* ». Chargé d'émancipations possibles autant qu'il est lourd d'asservissements potentiels, l'âge numérique appelle ce sursaut démocratique.

Car à l'enthousiasme des deux dernières décennies et à l'explosion des usages plébiscités sont venus s'ajouter le « blues » numérique, devant des phénomènes mondiaux et nationaux très inquiétants, et le « bluff » technologique, quand des solutions à tous les problèmes de la planète semblent surgir des laboratoires. **Les bienfaits s'effacent-ils désormais devant les menaces ?**

Snowden, ou la surveillance de masse. *Google*, ou l'hégémonie des plateformes géantes. *Uber*, ou l'explosion accélérée des modèles économiques et sociaux. Et bien d'autres changements sont à venir que le *big data*, les objets connectés, les nanotechnologies et biotechnologies font entrevoir. Ce n'est pas un autre monde, c'est le nôtre.

L'âge numérique met en scène le combat pluriséculaire qui oppose émancipation et domination. Il serait naïf de ne pas entendre l'alerte de M. Alain Supiot, ainsi résumée : « *la révolution numérique va ainsi de pair avec celle qui se donne à voir en matière juridique, où l'idéal d'une gouvernance des nombres tend à supplanter celui du gouvernement par les lois* » [(1)].

*

* *

L'extension des droits et des libertés exige donc pour l'avenir une puissante impulsion collective.

L'écosystème de l'internet français porte un optimisme créatif et lucide. Une vision résolument positive et progressiste se construit en France. Il

---

(1) Alain Supiot, La Gouvernance par les nombres – Cours au Collège de France *(2012-2014).*

faut le comprendre et le défendre. Les travaux récents du Conseil national du numérique et du Conseil d'État, mais aussi ceux de notre Commission, divergent parfois, convergent sur bien des points et souvent s'enrichissent mutuellement.

L'élaboration de la future loi française sur le numérique doit s'en emparer. Le législateur, s'il n'ignore rien des enjeux de l'économie numérique pour la France, ne saurait confiner le numérique à l'économie.

Le numérique doit **renforcer les conditions d'exercice de la liberté d'expression**, grâce aux nouveaux moyens de diffusion et de partage offerts par internet et au régime juridique équilibré de la loi pour la confiance dans l'économie numérique de 2004. Or, l'on a assisté depuis deux ans à la remise en cause progressive de cette liberté, au prétexte du renforcement de la lutte contre la prolifération des contenus illégaux : recours croissant au blocage administratif, sortie de certaines infractions de presse de la loi de 1881 sur la liberté de la presse, création de circonstances aggravantes à raison de l'utilisation d'internet, etc. Ces régressions sont d'autant plus regrettables qu'elles interviennent alors qu'il y a encore quelque mois, le 11 janvier 2015, des millions de Français défilaient dans les rues pour rappeler leur attachement à la préservation de cette liberté ancienne qui constitue, aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen, l'« *un des droits les plus précieux de l'Homme* », y compris voire surtout lorsqu'elle déplaît ou choque.

Par ailleurs, et alors que **les révélations de M. Edward Snowden auraient dû conduire à une réaction collective plus forte et à l'adoption d'un cadre juridique complet et solide pour les activités de surveillance administrative**, le Parlement français a manqué l'occasion qui lui était donnée de mettre un terme aux soupçons de surveillance massive et indiscriminée de la part des services de renseignement. Quoique porteuse d'avancées dans l'encadrement des activités de ces services, la loi relative au renseignement adoptée le 24 juin 2015 procède à un élargissement significatif des moyens mis à leur disposition et des finalités pour lesquelles ils peuvent être utilisés, aux dépens des exigences de proportionnalité et de subsidiarité. Ce faisant, elle autorise le recours à des méthodes de surveillance particulièrement intrusives pour la vie privée des individus, par exemple la mise en œuvre sur les réseaux de dispositifs algorithmiques destinés à détecter une menace terroriste (« boîtes noires »).

À cette position de méfiance, voire de défiance, à l'égard des technologies numériques et à leur instrumentalisation à des fins de surveillance, s'ajoute la relative inertie du législateur devant des décisions chaque jour plus urgentes. Tel est le cas **du droit à l'information publique**, dont le cadre juridique n'a quasiment pas changé depuis 1978 et se trouve fragilisé par la culture administrative française. Comme pour la liberté d'expression**, la révolution numérique fait levier pour rendre effectif le droit de savoir**, avec une ambition nouvelle. Elle déverrouille l'accès à des informations publiques désormais ouvertes.

Il en va de même de **la neutralité du net,** menacée par les logiques propres à l'écosystème numérique de plus en plus marqué par la centralisation de l'architecture des réseaux et la concentration verticale de leurs acteurs, et des « biens communs », expression qui désigne le modèle de partage et de gestion collective des ressources numériques.

La maîtrise de nos vies dépendra de l'usage et de la protection des données personnelles.

L'ampleur des transformations à l'œuvre a de longues date conduit à créer des lois protectrices, comme depuis 1978 la loi dite « Informatique et libertés », dont les principes fondateurs ont largement tenu face aux chocs.

Chacun s'accorde pour considérer que les protections ne se résument pas à celles que la loi installe et que les tribunaux veillent à appliquer. Depuis vingt ans, sur les réseaux, les pratiques de régulation sont multiformes : création des autorités administratives indépendantes, autorégulation et corégulation, responsabilité, formation et capacité des internautes, rôle actif d'innombrables communautés. La dimension internationale de la gouvernance et de la régulation est essentielle, tant l'application du droit est défiée par la liberté planétaire des réseaux.

Le champ des données personnelles a changé de dimension depuis 1978. Que faire ? Notre Commission est convaincue que **l'approche traditionnelle fondée sur la protection « passive » des individus** face aux activités des responsables de traitements, qu'ils soient privés ou publics, ne peut suffire à restaurer la confiance dans la société numérique, tant il reste encore beaucoup à faire pour écarter tout risque de surveillance interpersonnelle et institutionnelle. Certes, une forte logique de protection doit continuer de présider à l'encadrement des activités de surveillance administrative et judiciaire des pouvoirs publics, afin de mieux concilier les nécessités qui s'attachent à la préservation de l'ordre public et les droits de chacun au respect de son intimité.

Mais, au-delà, la Commission appelle à l'instauration d'**une logique d'autonomisation de l'individu sur les réseaux** afin de le doter des outils nécessaires à son épanouissement numérique. L'heure est venue de responsabiliser davantage chacune des parties prenantes de la société : le responsable de traitement, qui ne doit plus seulement se conformer *in abstracto* à des obligations légales mais s'inscrire davantage dans une démarche de responsabilisation (*accountability*) en démontrant à ses clients l'importance qu'il accorde à la préservation de leurs droits afin de mériter leur confiance ; et l'individu, qui doit être en mesure de s'autodéterminer dans l'univers numérique, en délivrant un consentement éclairé et effectif au traitement de ses données et en exerçant son libre arbitre et son libre agir, notamment face aux algorithmes prédictifs.

La vie commune dans le monde commun numérique.

Le monde numérique redonne des possibilités nouvelles à un monde commun. Cette perspective ambitieuse et réaliste à la fois permet de dépasser la simple distinction entre l'État et le marché.

Dans un moment où l'on s'interdit trop souvent de penser positivement l'avenir, d'imaginer des transformations qui soient autant de progrès, il y a là un gisement considérable. Internet n'existerait pas sans le modèle coopératif qui a permis sa création et ses développements, par le partage de ressources mises en commun. **Dans cet univers il existe des ressources libres qui sont celles mises « *à la disposition de tout le monde* »** [(1)].

L'existence des communs de la connaissance et de l'information en réseau permet de nouvelles formes de partage, elle ne suffit pas à elle seule à les rendre effectives.

Des choix politiques et juridiques s'imposent pour **déterminer les nouveaux droits ou les capacités d'usage de l'information et de la connaissance à l'âge numérique**. Les enjeux sont immenses. Selon les choix qui seront faits, la création et la circulation des œuvres et des connaissances ainsi que le partage de la valeur prendront des directions différentes. Une nouvelle impulsion doit être donnée pour fluidifier l'accès et la diffusion de la culture et garantir ainsi le respect du pluralisme. L'accès aux œuvres culturelles et leur diffusion seront transformés, ou, à l'inverse, des batailles de retardement figeront longtemps encore des rapports dépassés.

Acceptons l'idée que nous vivons une nouvelle Renaissance, par l'ampleur des innovations en cours. Et recherchons **un nouveau compromis** entre les droits en présence comme on a su le faire de Beaumarchais à nos jours.

La stratégie juridique.

La révolution numérique exerce une forte pression sur la production de la norme de droit. **L'Union européenne y prend toute sa place**, tant l'espace national apparaît étroit. Le très récent compromis sur la neutralité des réseaux (« *pour garantir l'accès à un internet ouvert* ») entre le Parlement européen, le Conseil et la Commission, pour un règlement d'application immédiate, montre une nouvelle fois l'importance et l'impact de la législation européenne. Mais celle-ci se nourrit également des débats nationaux. **Le présent rapport a aussi pour vocation d'inspirer le débat européen.**

---

(1) Lawrence Lessig, L'Avenir des idées, *Broché, 2005.*

Au carrefour des compétences exclusives (règles de concurrence nécessaires au fonctionnement du marché intérieur) [1] et partagées avec les États membres (marché intérieur, protection des consommateurs, réseaux transeuropéens des télécommunications, espace de liberté, de sécurité et de justice …) [2] dont dispose l'Union européenne, **le numérique irrigue nombre des politiques et des normes communautaires depuis près de vingt ans** : ouverture des données publiques [3], protection des données personnelles [4], marché unique des télécommunications [5], produits audiovisuels [6], certains aspects particuliers des droits de propriété intellectuelle [7]…

Depuis la stratégie numérique pour l'Europe adoptée en 2010 [8], l'Union européenne souhaite approfondir les actions entreprises jusque-là en matière de marché unique numérique afin que les citoyens et les entreprises tirent le meilleur parti des technologies numériques. Cette stratégie, qui repose sur l'approfondissement de l'harmonisation des normes applicables en la matière, conduit parfois à l'adoption de règlements de portée générale ne nécessitant aucune transposition par le législateur national, en complément ou en remplacement des directives adoptées par le passé. Il en va ainsi en matière de protection des données personnelles [9], avec l'adoption prochaine du projet de règlement général sur la protection des données en remplacement de la directive de 1995, ou en matière de régulation du marché des télécommunications, avec l'adoption prochaine du projet de règlement établissant des mesures relatives au

---

(1) En application du b *du 1 de l'article 3 du traité sur le fonctionnement de l'Union européenne (TFUE).*

(2) En application du 2 de l'article 4 du TFUE.

(3) Directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

(4) Directive 95/46/CE 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 et décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

(5) Directive 2002/20/CE du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques, directive 2002/19/CE du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, directive 2002/22/CE du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, règlement (CE) n° 1211/2009 du 25 novembre 2009 instituant l'Organe des régulateurs européens des communications électroniques (ORECE) ainsi que l'Office et règlement (UE) n° 531/2012 du 13 juin 2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union.

(6) Directive 2010/13/UE du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels.

(7) Directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

(8) http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:si0016.

(9) L'article 16 du TFUE reconnaît à toute personne le « droit à la protection des données à caractère personnel la concernant *» et donne compétence au Parlement européen et au Conseil pour fixer «* les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données ».

marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté.

Pour ce qui relève des choix politiques de la France, il reste à décider **si quelques-uns des principes de l'âge numérique doivent être défendus dans nos lois, ou être érigés au rang de principes fondamentaux de valeur constitutionnelle**. Notre Commission considère à ce titre qu'il conviendrait d'inscrire explicitement dans la Constitution les droits au respect de la vie privée et à la protection des données à caractère personnel afin de rehausser l'importance accordée à ces principes fondamentaux en droit interne. À l'avenir, d'autres principes, comme la neutralité, pourront rejoindre le bloc de constitutionnalité.

Cinq familles de propositions.

Loin de se résigner aux évolutions les plus récentes et convaincue que le numérique est au contraire porteur d'un mouvement de progrès et d'approfondissement des droits, **la Commission a concentré ses réflexions et ses propositions sur cinq problématiques** qui traduisent bien l'ambivalence de la révolution numérique et les tensions qui l'animent.

Elle estime, en tout premier lieu, que le numérique doit être l'occasion de **prolonger d'anciennes et essentielles conquêtes démocratiques,** que sont en particulier **la liberté d'expression et de communication**, dans sa double dimension relative au droit à l'information et à la libre expression des opinions, et **le droit à la vie privée**.

S'agissant du droit à l'information, la Commission s'est interrogée sur les moyens d'**améliorer les conditions dans lesquelles il est possible d'accéder à l'information d'intérêt public** : pour ce faire, elle préconise de reconnaître par la loi un véritable « droit de savoir » à l'ère numérique, passant par la consécration d'un droit fondamental à l'information publique, l'inscription dans notre droit du principe d'ouverture des données publiques (*open data*) et le renforcement de la protection des lanceurs d'alerte (**I**).

La Commission a également recherché la manière de **mieux concilier la défense de la liberté d'expression avec l'exigence de lutte contre les contenus illégaux sur internet** : après avoir rappelé que l'univers numérique ne saurait faire l'objet d'un régime dérogatoire en la matière, conformément au principe de neutralité technologique, elle recommande de préserver l'esprit et la portée de la loi du 29 juillet 1881 sur la liberté de la presse, aujourd'hui mise à mal, et de conforter le rôle du juge judiciaire dans la mise en œuvre de la liberté d'expression (**II**).

Ensuite, la Commission considère que le numérique oblige à **repenser les contours et les modalités d'exercice du droit fondamental au respect de la vie privée**, condition essentielle de l'autonomie individuelle. S'il faut réévaluer l'importance accordée à la vie privée ainsi qu'à son avatar numérique, la protection des données à caractère personnel, il convient également de renforcer la

maîtrise et l'autodétermination de l'individu sur son existence numérique en renforçant son libre arbitre et sa liberté d'agir sur les réseaux. Face aux risques d'ingérence de la puissance publique dans la sphère intime, il apparaît nécessaire de mieux concilier les nécessités de préservation de l'ordre public et la protection de la vie privée (**III**).

Enfin, la Commission a analysé les questions *« digital natives »*, nées avec les réseaux numériques, et s'est attachée à **dégager les principes nécessaires à la vie commune dans la nouvelle société numérique**.

Il importe en effet de **déterminer de nouvelles garanties indispensables à l'exercice des libertés fondamentales à l'âge numérique**, parmi lesquelles figurent le droit d'accès à internet, la neutralité des réseaux et des dispositifs mobiles ainsi que la régulation des plateformes (**IV**).

Dans le contexte de la mise en réseau et du partage des compétences, des outils et des savoirs, cette conquête de nouveaux droits passe également par la redéfinition de la place de la propriété dans la société numérique, ce qui implique de **dessiner une nouvelle frontière entre propriété et communs** (**V**).

La responsabilité du Parlement, pour l'avenir.

Les travaux de notre Commission ont débuté après son installation par M. Claude BARTOLONE le 11 juin 2014.

En effet, devant les enjeux immenses que provoque la révolution numérique, **les réponses parlementaires ne peuvent rester en l'état** : des législations au fil de l'eau, une délibération collective insuffisante et contrariée par la puissance des lobbys, et plus grave, des choix contestables qui créent des brèches durables, affaiblissant les libertés individuelles et collectives.

Dix-huit mois après la décision de créer cette Commission, **la situation dans notre pays s'est aggravée**. Avant même l'achèvement de nos travaux, les discussions sur la loi relative au renseignement témoignent de l'étendue des risques. **Notre Commission s'est exprimée à plusieurs reprises, à l'unanimité, pour faire entendre que les lois récentes créent un effet de brèche** qui en rendra possibles d'autres. Nous plaidons pour éviter à la France un renoncement démocratique, un malentendu historique douteux et coûteux à propos de l'internet. Les réseaux numériques ne sont pas hors du droit. Aussi ne cédons pas à la tentation, année après année, de leur appliquer des lois d'exception [(1)].

Et pour l'avenir ? Une commission constituée pour une durée déterminée n'a pas vocation de proposer elle-même sa transformation automatique en organisme permanent. Notre Commission échappera donc à cette tentation.

---

(1) Voir la recommandation du 22 juillet 2014 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, la recommandation du 29 septembre 2014 sur plusieurs articles du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme et la recommandation du 1er avril 2015 sur le projet de loi relatif au renseignement.

Il demeure que l'omniprésence du numérique et son impact dans tous les domaines de la société et de l'action publique devront provoquer une réflexion institutionnelle au sein des Parlements, en Europe comme ailleurs. **L'absence d'une culture numérique forte affaiblit la qualité des choix politiques et législatifs actuels.** À l'instar des évolutions produites par la prise de conscience à l'égard de l'écologie et du développement durable, **l'Assemblée nationale doit se doter d'une organisation capable d'affronter les défis parmi les plus redoutables de la modernité,** en alliant le meilleur de la technique et de la tradition démocratique. Le défi numérique appelle une adaptation sans retard du travail parlementaire.

Ce rapport, issu d'une commission inédite à l'Assemblée nationale dans sa composition, démontre par ailleurs **l'intérêt d'expérimenter des formes démocratiques nouvelles pour défricher des questions complexes**, dépassant les clivages traditionnels, sans pour autant se satisfaire de faux consensus.

Remerciements.

Le président de l'Assemblée nationale Claude Bartolone a voulu cette commission, et lui a donné les moyens de travailler librement, dans des conditions exceptionnelles.

La Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, a réuni, pour la première fois dans l'histoire de l'Assemblée, treize députés de la majorité et de l'opposition [(1)] et treize personnalités qualifiées. Elle a ainsi rassemblé des universitaires et experts, un journaliste, des praticiens du droit et des entrepreneurs [(2)], sous la coprésidence de M. Christian Paul, député du groupe Socialiste, républicain et citoyen, et de Mme Christiane Féral-Schuhl, avocate, ancienne bâtonnière de Paris.

La Commission a procédé à près de vingt-cinq séances d'auditions ; elle a également rencontré à plusieurs reprises le Conseil national du numérique. Elle a effectué, le 5 mars 2015, un déplacement à Bruxelles afin de suivre au plus près l'évolution des discussions sur les principaux textes communautaires qui intéressent le numérique. Après avoir échangé sur la stratégie numérique de l'Union européenne avec M. Andrus Ansip, vice-président de la Commission européenne chargé du marché unique du numérique, elle a rencontré des représentants du Parlement européen, du Conseil de l'Union européenne et de la Commission européenne.

---

(1) *Patrick Bloche (Socialiste, républicain et citoyen), Sergio Coronado (Écologiste), Charles de Courson (Union des démocrates et indépendants), Virginie Duby-Muller (Les Républicains), Laurence Dumont (Socialiste, républicain et citoyen), Corinne Erhel (Socialiste, républicain et citoyen), Gilda Hobert (Radical, républicain, démocrate et progressiste), Laure de La Raudière (Les Républicains), Martine Martinel (Socialiste, républicain et citoyen), Christian Paul (Socialiste, républicain et citoyen), Franck Riester (Les Républicains), Gabriel Serville (Gauche démocrate et républicaine) et Patrice Verchère (Les Républicains).*

(2) *Philippe Aigrain, Godefroy Beauvallet, Valérie-Laure Benabou, Jean Dionis du Séjour, Christiane Féral-Schuhl, Daniel Le Métayer, Winston Maxwell, Francesca Musiani, Edwy Plenel, Myriam Quemener, Thaima Samman, Henri Verdier et Cyril Zimmermann.*

Elle a enfin travaillé avec la Chambre des députés italienne à l'élaboration d'**une déclaration commune des droits sur internet** que les présidents des deux Assemblées ont signée à Paris le 28 septembre 2015.

Que celles et ceux qui ont participé à ces travaux, les ont accompagnés ou enrichis en soient très sincèrement remerciés. Ce rapport a largement bénéficié de la haute compétence et de la présence précieuse des administrateurs de l'Assemblée nationale.

I. RENFORCER LE DROIT À L'INFORMATION À L'ÈRE NUMÉRIQUE

En démocratie, où, pour reprendre la formule lancée en août 1789 par Jean Sylvain Bailly, premier président du tiers état et maire de Paris, « *la publicité de la vie politique est la sauvegarde du peuple* » (1), tout individu doit pouvoir accéder aux informations d'intérêt public pour agir en citoyen, apprécier les conditions dans lesquelles les affaires publiques sont gérées et participer à la vie démocratique et au débat d'opinion.

Le numérique, trop souvent appréhendé négativement ou présenté comme une atteinte aux libertés individuelles, renouvelle les conditions dans lesquelles les exigences anciennes de transparence et de redevabilité publiques se concrétisent. Il offre en effet aux autorités publiques la possibilité de mettre à la disposition du plus grand nombre les informations d'intérêt public.

En France, la publication de ces informations procède de deux principes fondamentaux, protégés par les articles 11 et 15 de la Déclaration des droits de l'homme et du citoyen de 1789 : d'une part, la liberté d'expression et de communication, selon laquelle « *tout Citoyen peut (...) parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi* » et, d'autre part, les exigences de contrôle et de responsabilité des agents publics, qui impliquent que « [l]*a Société a le droit de demander compte à tout Agent public de son administration* ».

Dans notre pays, où la culture administrative a été fortement marquée par la tradition du secret et de la confidentialité, la liberté de s'informer des affaires publiques a été consacrée tardivement et concrétisée partiellement par la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, dont le chapitre Ier porte sur la « *liberté d'accès aux documents administratifs et (...) la réutilisation des informations publiques* » et l'article 1er protège « *le droit de toute personne à l'information* ».

Cette liberté s'est peu à peu adaptée à la révolution technologique de la dématérialisation et aux modifications des conditions techniques de diffusion des informatiques publiques. Elle s'exerce aujourd'hui selon trois modalités principales, complémentaires mais d'inégale portée :

– un droit d'accès ponctuel et à la demande permettant à toute personne, depuis 1978, d'obtenir la communication de documents administratifs (information « *quérable* » (2)) ;

---

(1) Cité par Jean-Noël Jeanneney, Une histoire des médias, des origines à nos jours, *Paris, Seuil, 1996, p. 60.*

(2) Commissariat général du plan (Dieudonné Mandelkern, Bertrand du Marais), Diffusion des données publiques et révolution numérique, *décembre 1999, p. 14.*

– avec le développement d'internet dans les années 2000, la possibilité pour chacun de consulter l'information publique diffusée par l'administration sans en formuler la demande préalable (information « *portable* » [1]) ;

– à partir de 2011 et de l'essor des techniques de traitements informatiques de données brutes, un droit de réutilisation des données publiques mises en ligne (information *réutilisable*).

Face au caractère incomplet et partiel de chacun de ces droits, la Commission recommande de substituer à la logique actuelle une ambition plus grande visant à l'instauration d'un véritable droit à l'information publique (**A**). Corrélativement, elle suggère de renforcer l'effectivité de ce nouveau droit par une meilleure mobilisation des possibilités permises par le numérique en améliorant les conditions de communication et de réutilisation des informations publiées (**B**). Enfin, elle souhaite relancer la réflexion sur la création d'un statut protecteur des lanceurs d'alerte sans lequel il ne lui paraît pas possible de garantir la publication de certaines informations sensibles (**C**).

A. CONSACRER UN DROIT FONDAMENTAL À L'INFORMATION D'INTÉRÊT PUBLIC

À l'issue de plusieurs auditions sur le sujet, en particulier celles de Mme Corinne Bouchoux, rapporteure d'une mission d'information du Sénat sur l'accès aux documents administratifs et aux données publiques [2], de M. Serge Daël, alors président de la Commission d'accès aux documents administratifs (CADA) [3], ainsi que de MM. Henri Verdier, directeur d'Étalab et Mohammed Adnène Trojette, auteur en 2013 d'un rapport consacré à l'*open data* [4], la Commission constate que les conditions d'accès aux informations publiques sont, en France, peu satisfaisantes : la liberté d'accéder aux documents administratifs reconnue en 1978 demeure conditionnée et entravée (**1**) et n'a pas été confortée par une politique ambitieuse de diffusion numérique et d'ouverture des données publiques (**2**). En conséquence, elle recommande de bouleverser la logique du droit existant en procédant à la consécration juridique d'un véritable droit à l'information d'intérêt public (**3**).

1. Un droit d'accès aux documents administratifs ancien mais conditionné et inabouti

Il n'existe pas, en France, de véritable droit à l'information publique mais seulement un droit individuel d'accès aux documents administratifs et « à la

---

(1) Ibid.

(2) Rapport d'information (n° 589, session ordinaire de 2013-2014) de Mme Corinne Bouchoux au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques du Sénat, juin 2014.

(3) Audition de Mme Corinne Bouchoux et M. Serge Daël du 9 juillet 2014.

(4) Audition de MM. Henri Verdier et Mohammed Adnène Trojette du 1er octobre 2014.

demande » qui s'exerce de manière conditionnée (***a***) et demeure, à maints égards, inabouti (***b***).

a. Un droit d'accès individuel et « à la demande » conditionné

La loi n° 78-753 du 17 juillet 1978 précitée s'est en partie inspirée des principes et de la logique qui avaient présidé, quelques mois plus tôt, à l'adoption de la loi fondatrice en matière de protection des données personnelles, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et libertés ». Elle a ainsi octroyé un droit d'accès de l'individu aux documents administratifs et institué une autorité administrative indépendante chargée de veiller à sa bonne application, la CADA. Ce droit est ouvert à toute personne et concerne **tout document détenu par l'administration**, qu'il ait été produit ou reçu par elle.

Sur le plan pratique, le droit d'accès « *s'exerce, au choix du demandeur et dans la limite des possibilités techniques de l'administration* » par consultation gratuite sur place, par la délivrance d'une copie aux frais du demandeur si la reproduction du document est possible ou par courrier électronique et sans frais lorsqu'il est disponible sous format électronique [(1)]. La CADA exerce un rôle précontentieux et consultatif, préalable obligatoire à l'exercice ultérieur d'un éventuel recours devant le juge administratif [(2)] : saisie par l'administré dans les deux mois suivant le refus de communication de l'administration, elle formule un avis dans un délai d'un mois sur la communicabilité du document que l'administration n'est cependant pas tenue de suivre.

L'article 1er de la loi n° 78-753 du 17 juillet 1978 précitée dispose que « *sont considérés comme documents administratifs, (…) quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions et décisions* ».

Un large spectre de documents est ainsi concerné mais leur communication est **soumise à plusieurs conditions** qui en limitent sensiblement la portée.

Tout d'abord, les documents dont la communication est sollicitée doivent être achevés, ne pas constituer des documents préparatoires à une décision

---

(1) Article 4 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

(2) Article 20 de la même loi.

administrative toujours en cours d'élaboration et ne pas avoir fait l'objet d'une diffusion publique [1].

En outre, de nombreuses exceptions font obstacle à l'exercice du droit d'accès ou en réduisent la portée. Certains documents ne sont pas communicables, soit en raison de leur nature même (avis des juridictions administratives, rapports de contrôle de la Cour des comptes ou des chambres régionales des comptes, documents élaborés ou détenus par l'Autorité de la concurrence dans ses pouvoirs d'enquête, d'instruction et de décision, documents élaborés ou détenus par la Haute Autorité pour la transparence de la vie publique, documents préalables à l'accréditation des établissements et personnels de santé et leurs rapports d'audit [2]), soit en raison des secrets et intérêts protégés par la loi, lesquels ne peuvent toutefois justifier que l'occultation ou la disjonction des seules mentions protégées (délibérations du Gouvernement, défense nationale, politique extérieure de la France, sûreté de l'État, sécurité publique et sécurité des personnes, monnaie et crédit public, déroulement des procédures devant les juridictions, recherche des infractions fiscales ou douanières [3]).

De surcroît, ne sont communicables qu'à l'intéressé – personne physique ou morale – les documents dont la publication porterait atteinte à la protection de sa vie privée, au secret médical ou au secret en matière commerciale et industrielle, portant une appréciation ou un jugement de valeur sur son comportement ou le faisant apparaître dans des conditions susceptibles de lui porter préjudice [4].

Enfin, plusieurs documents ne sont communicables qu'à l'issue d'un certain délai : il en va ainsi des actes préparatoires à une décision, communicables une fois que la décision a été prise (sauf les documents d'urbanisme ou d'installations classées pour la protection de l'environnement), et des archives publiques, auxquelles s'appliquent des délais variables selon leur sensibilité, allant de vingt-cinq à cent ans [5].

b. Un droit d'accès inabouti

La Commission reconnaît que **d'importants progrès ont été accomplis en matière d'accès aux documents administratifs depuis 1978**. Comme l'ont souligné devant elle Mme Corinne Bouchoux et M. Serge Daël, le rôle de la CADA, bien que purement consultatif, a été positif dans la mise en œuvre pratique de cette liberté. Ses avis, précisément documentés et motivés, sont généralement confirmés par le juge. Son approche pédagogique et incitative est saluée, grâce au rôle joué, en interne, par les personnes responsables de l'accès au sein des administrations (PRADA). Conjointement avec le juge administratif, elle a

---

(1) Article 2 de la même loi.

(2) 1° du I de l'article 6 de la même loi.

(3) 2° du même I.

(4) II du même article.

(5) Articles L. 213-1 à L. 213-8 du code du patrimoine.

interprété les dispositions de la loi de 1978 dans un sens favorable à l'accès des citoyens, en vidant largement de sa portée juridique la notion de documents internes non communicables, en limitant significativement la durée d'opposabilité du caractère préparatoire d'un document et en élargissant la communication des documents à tout type de support, y compris les bases de données, afin de tirer les conséquences de leur dématérialisation (1).

Toutefois, l'exercice du droit d'accès se heurte à au moins **quatre obstacles** (2) :

– en tout premier lieu, la lenteur des administrations dans la communication des documents demandés et dans la transmission des archives, certains délais pouvant atteindre vingt mois en cas de refus persistant (3) ;

– en deuxième lieu, l'interprétation extensive développée par les administrations des exceptions au droit de communication, notamment lorsqu'est en cause le secret de la vie privée ou le secret commercial et industriel, comme en témoigne le nombre important d'avis formulés chaque année par la CADA – près de 5 300 en 2013 – et sa stabilisation à un niveau élevé depuis plusieurs années (4) ;

– en troisième lieu, les difficultés rencontrées par l'administré dans l'identification du document pertinent – en raison du caractère incomplet et imprécis du répertoire des principaux documents administratifs mis à sa disposition pour le guider – et du service compétent – l'obligation faite à l'administration saisie de transférer la demande au service compétent n'étant pas toujours respectée ;

– en quatrième et dernier lieu, l'existence, à côté de la loi n° 78-753 du 17 juillet 1978 précitée, de régimes particuliers ou autonomes de communication de documents administratifs : certains d'entre eux, initialement autonomes, ont été progressivement alignés sur le droit commun (5) mais d'autres demeurent totalement autonomes, comme l'accès aux éléments de calcul de l'impôt sur le revenu (6), la consultation des déclarations de situation patrimoniale des parlementaires (7), le droit à l'information des élus municipaux (8) ou la diffusion

---

(1) Voir le rapport d'information (n° 589, session ordinaire de 2013-2014), op. cit., *pp. 73-80.*

(2) Ibid.

(3) Un mois est octroyé à l'administration pour répondre à la demande du citoyen (contre vingt jours par exemple au Royaume-Uni) ; en cas de refus de communication, la CADA statue en un mois ; en cas de refus persistant, un délai de deux mois est laissé au demandeur pour saisir le tribunal administratif qui statue en moyenne en dix-sept mois.

(4) CADA, Rapport d'activité 2013, *pp. 66-82.*

(5) Ils sont recensés par l'article 21 de la loi n° 78-753 du 17 juillet 1978 précitée.

(6) Article L. 111 du livre des procédures fiscales.

(7) Article L.O. 135-2 du code électoral.

(8) Article L. 2121-13 du code général des collectivités territoriales.

des informations environnementales qui font, elles, l'objet d'un droit d'accès élargi et renforcé [1].

2. L'absence d'offre globale et satisfaisante d'informations publiques

Si l'État s'est en partie adapté aux évolutions technologiques et a encouragé la diffusion de l'information publique (***a***) puis l'ouverture des données publiques à des fins de réutilisation (***b***), aucune de ces deux politiques de communication n'est venue corriger de manière totalement satisfaisante les insuffisances du droit d'accès.

a. Une diffusion croissante mais partielle des informations publiques

Le droit traditionnel d'accès aux documents administratifs s'est prolongé, à partir des années 2000, par une **politique de communication plus large des documents administratifs consistant dans la diffusion de l'information publique sans demande préalable**, principalement dans le but de renforcer la liberté d'accès aux règles de droit applicables aux citoyens.

Dans cet esprit, « *la mise à disposition et la diffusion des textes juridiques constituent une mission de service public au bon accomplissement de laquelle il appartient aux autorités administratives de veiller* » [2] : ce sont notamment les missions confiées au *Journal officiel de la République française*, à *Légifrance* ou à *BOFIP-Impôts*. L'article 7 de la loi n° 78-753 du 17 juillet 1978 précitée rend obligatoire la publication des directives, instructions, circulaires, notes et réponses ministérielles « *qui comportent une interprétation du droit positif ou une description des procédures administratives* ». Doivent également être publiés les actes [3], les documents et les délibérations [4] des collectivités territoriales, certains documents environnementaux (information préalable à une consultation du public [5], informations générales, etc.), les répertoires des principaux documents existants afin de faciliter l'exercice du droit d'accès [6] ou les déclarations d'intérêts et de patrimoine de certains responsables publics [7].

Conformément aux exigences de protection des données personnelles, la diffusion d'une information publique est subordonnée à un traitement préalable afin « *d'occulter* [l]*es mentions* [portant sur la vie privée] *ou de rendre impossible l'identification des personnes qui y sont nommées* » [8].

---

(1) Articles L. 124-1 à L. 124-8 du code de l'environnement.

(2) Article 2 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

(3) Articles L. 2131-1, L. 3131-1 et L. 4141-1 du code général des collectivités territoriales.

(4) Articles L. 2121-24, L. 2121-25, L. 2313-1, L. 3313-1 et L. 4313-1 du même code.

(5) Articles L. 123-10, L. 122-1-1, L. 122-8, L. 124-7, L. 124-8, L. 127-1 à L. 127-10 et R. 124-5 du code de l'environnement.

(6) Article 17 de la loi n° 78-753 du 17 juillet 1978 précitée.

(7) Articles 5 et 12 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique.

(8) Avant-dernier alinéa de l'article 7 de la loi n° 78-753 du 17 juillet 1978 précitée.

Au terme des auditions qu'elle a conduites, la Commission est convaincue que **la diffusion de l'information publique a amélioré l'information des citoyens, notamment dans un souci de transparence administrative**, en leur fournissant des outils pédagogiques et en facilitant leurs recherches, par la création de profils d'utilisateurs, la mise en place de moteurs de recherche, l'ouverture de portails de référence ainsi que par une catégorisation et une indexation accrues de l'information. **Toutefois, cette politique n'a pas permis de suppléer totalement les insuffisances du droit d'accès ponctuel et à la demande aux documents administratifs**. L'information disponible apparaît encore difficile à identifier, lacunaire, de qualité inégale et parfois inadaptée aux attentes des citoyens, des journalistes, des chercheurs ou des entreprises : certains documents fréquemment demandés demeurent absents des sites administratifs tandis que d'autres, qui sont mis en ligne, sont dispersés à plusieurs endroits, publiés dans un format rigide ou instable et insuffisamment mis à jour (1).

Au-delà de ces difficultés pratiques, la Commission regrette le caractère partiel de l'offre d'informations diffusées et relève que, hors les cas où la loi l'a rendue obligatoire, la publication des informations produites ou reçues par l'administration est demeurée facultative (2).

b. Un mouvement d'ouverture des données publiques dynamique mais encore à ses débuts

En prolongement de cette politique a été lancée, à partir de 2011 (3), une démarche d'**ouverture des données publiques** (*open data* (4)) qui puise toutefois ses racines dans des initiatives plus anciennes (voir l'encadré ci-après). Elle consiste à **mettre à la disposition de tiers les informations publiques dans des formats en permettant la réutilisation par une machine à un ensemble de fins non limitativement énumérées** et sur lesquelles s'exerce un droit de libre usage.

Les origines du mouvement d'ouverture des données publiques en France

Le 25 août 1997, le Premier ministre, M. Lionel Jospin, a eu l'occasion de souligner que « *depuis près de vingt ans, l'accès aux documents administratifs est devenu une véritable liberté publique ; aujourd'hui, la technologie facilite les conditions de leur diffusion. Les données publiques essentielles doivent désormais pouvoir être accessibles à tous gratuitement sur internet* ».

Plus tard, le rapport de MM. Dieudonné Mandelkern et Bertrand du Marais intitulé *Diffusion des données publiques et révolution numérique* (décembre 1999) percevait déjà les

---

(1) Voir le rapport d'information (n° 589, session ordinaire de 2013-2014), op. cit.*, pp. 94-99.*

(2) Avant-dernier alinéa de l'article 7 de la loi n° 78-753 du 17 juillet 1978 précitée.

(3) Toutefois, dès le 20 octobre 2008, la France a présenté un plan « France Numérique 2012 » visant à « favoriser la réutilisation des informations publiques par les agents économiques *», notamment par la création d'un portail unique d'accès aux données publiques (action n° 39).*

*(4) Le concept d'*open data *remonte au milieu des années 1990 lorsque des chercheurs ont plaidé pour l'ouverture et le partage des résultats de leurs travaux portant sur des données géophysiques et environnementales afin de tenir compte du caractère transfrontière des phénomènes étudiés et de se prémunir contre toute privatisation des connaissances.*

données publiques et leur diffusion à titre gratuit comme un levier de la stratégie d'influence du Gouvernement.

Le programme d'action gouvernemental pour la société de l'information (PAGSI) adopté en janvier 1998 prévoyait ainsi la diffusion des « *données publiques essentielles* », comme « *les grands textes de notre droit, l'information administrative du public, les principaux documents publics et des données culturelles essentielles* ». Ce programme devait être concrétisé dans le projet de loi sur la société de l'information, enregistré à la Présidence de l'Assemblée nationale le 14 juin 2001, qui introduisait un nouvel article 15 dans la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal prévoyant notamment que « *les services et établissements publics administratifs de l'État mettent gratuitement à la disposition du public, sur des sites accessibles en ligne, les données essentielles qui la concernent. Ces données peuvent être gratuitement utilisées et rediffusées, y compris à des fins commerciales, à condition qu'elles ne subissent pas d'altération et que leur source soit mentionnée* ». Bien que ce texte n'ait jamais été adopté, cette vision politique a toutefois permis certaines avancées en la matière, comme la mise à disposition gratuite du *Journal officiel de la République française*, prévue par l'ordonnance n° 2004-164 du 20 février 2004 relative aux modalités et effets de la publication des lois et de certains actes administratifs.

Avec l'*open data*, l'obligation d'information du citoyen se double de l'ambition de libérer une capacité d'agir dans les sphères économique et sociale. La facilité technique et juridique d'usage de ces données, leur accessibilité et leur interopérabilité deviennent essentielles. Le droit à l'information se complète ainsi d'un effort pour **libérer des externalités positives** (comme dans l'*open data* en matière de transports) ou pour **développer des infrastructures de données essentielles** (référentiels géographiques par exemple).

La loi n° 78-753 du 17 juillet 1978 précitée a instauré sur les données mises en ligne par l'administration un droit de réutilisation. Ce droit porte sur l'ensemble des documents communicables à travers le droit d'accès et fait l'objet des mêmes exceptions et limitations, tenant notamment à la nécessité de protéger la vie privée ou le secret commercial et industriel [(1)]. Le droit à réutilisation d'une information publique contenant des données personnelles est soumis au recueil préalable du consentement de la personne concernée, à l'anonymisation par l'autorité détentrice – sous réserve qu'elle ne requière pas un effort disproportionné – ou à l'autorisation expresse d'une disposition législative ou réglementaire ; il doit également être conforme aux conditions posées par la loi dite « Informatique et libertés » en matière de licéité, de formalités préalables et de respect des droits d'opposition, d'information et de rectification [(2)].

Ne peuvent pas non plus faire l'objet d'une réutilisation les données des services publics industriels et commerciaux, sauf si l'établissement concerné décide volontairement de procéder à leur ouverture, les données sur lesquelles des

---

(1) Voir supra, *le* a *du 1 du présent A.*

(2) Article 13 de la loi n° 78-753 du 17 juillet 1978 précitée.

tiers détiennent des droits de propriété intellectuelle [(1)] – œuvres conservées par les musées [(2)], bases de données publiques dont la constitution, la vérification ou la présentation a requis un investissement financier, matériel ou humain substantiel [(3)], logiciels utilisés par l'administration et conçus par un tiers – et les données soumises à des droits d'exclusivité consentis par l'administration à des tiers [(4)].

À l'instar du droit d'accès aux documents administratifs, la CADA est compétente pour formuler un avis à la suite d'une décision défavorable de l'administration de rendre réutilisables certaines données. De plus, saisie par l'administration concernée, elle contrôle et sanctionne l'éventuel non-respect des conditions de cette réutilisation. L'ensemble des actions des administrations impliquées dans cette démarche est coordonné par la mission Étalab, qui pilote le site data.gouv.fr, portail unique hébergeant l'ensemble des données publiques ouvertes par l'État, lancé le 5 décembre 2011 [(5)].

La Commission estime que la logique qui préside à **l'*open data* parachève la liberté d'accès aux informations publiques en faisant passer** leurs modalités de communication **d'une « logique de demande »**, fondée sur l'obligation de communiquer des documents administratifs après que le citoyen en a formulé le souhait, **à une « logique d'offre »**, consistant dans la mise à disposition des documents publics dans des conditions en permettant l'exploitation et la réutilisation. De nombreuses bases de données ont été ouvertes, démarche qui s'est accompagnée de réels efforts de clarification, de simplification, d'indexation et de mise en relation des données brutes mises à disposition. Ces résultats ont aussi permis de constater combien étaient fortes les attentes et les exigences en la matière [(6)]. Avec 20 000 jeux de données disponibles sur data.gouv.fr, la France figure, depuis 2014, au troisième rang des pays du monde [(7)] et de l'Union européenne [(8)] les plus avancés dans la démarche d'*open data*. Elle a également été désignée pour présider, durant l'année 2016, le Partenariat pour le Gouvernement Ouvert (*Open Government Partnership*).

Ces **résultats** sont **encourageants**, notamment grâce au travail mené par la mission Étalab et à la création d'un poste d'administrateur général des données chargé de « *coordonne*[r] *l'action des administrations en matière d'inventaire, de gouvernance, de production, de circulation et d'exploitation des données par les administrations (…)* [et d']*organise*[r], *dans le respect de la protection des données personnelles et des secrets protégés par la loi, la meilleure exploitation*

---

(1) Article 10 de la même loi.

(2) Dans les conditions prévues par l'article L. 111-1 du code de la propriété intellectuelle.

(3) Article L. 341-1 du même code.

(4) Article 14 de la loi n° 78-753 du 17 juillet 1978 précitée.

(5) La création et la mise en ligne de ce portail furent décidées par le conseil de modernisation des politiques publiques du 30 juin 2010 et annoncées à l'issue du conseil des ministres du 24 novembre 2010.

(6) Voir le rapport d'information (n° 589, session ordinaire de 2013-2014), op. cit., *pp. 100-133.*

(7) Classement Global Open Data Index *par l'*Open Knowledge Foundation.

(8) Classement publié par PSIPlatform.

de ces données et leur plus large circulation, notamment aux fins d'évaluation des politiques publiques, d'amélioration et de transparence de l'action publique et de stimulation de la recherche et de l'innovation » [(1)].

La Commission observe **toutefois** que **l'ouverture des données publiques s'inscrit, en France, en dehors de toute obligation légale**, ce qui en réduit la portée et l'impact sur les conditions d'accès aux informations d'intérêt général, même si le législateur a prévu, à l'article 106 de la loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République, de rendre obligatoires, pour les collectivités territoriales de plus de 3 500 habitants et les établissements publics de coopération intercommunale à fiscalité propre auxquels elles appartiennent, la mise à disposition des données publiques dont elles disposent au format électronique sur leur site internet et leur libre réutilisation.

Le **cadre exclusivement volontariste et incitatif** dans lequel s'opère cette ouverture freine la diffusion de la culture de la transparence publique. Elle favorise la logique de silos propre à l'organisation administrative française : l'administration préfère conserver un pouvoir exclusif sur les informations qu'elle détient ou produit et n'est pas encouragée à former ses agents et à développer, en interne, les compétences requises.

Cette démarche se heurte au surplus à de **nombreuses difficultés techniques, méthodologiques et financières** qui font obstacle à la libre accessibilité et à la réutilisation gratuite et automatisée de l'ensemble des données publiées. Le recours à des formats, logiciels ou applications fermés bloque ou complique la communication, l'extraction et la réutilisation ultérieure de ces données. Le défaut de contextualisation, l'absence de présentation des choix méthodologiques retenus et les limites posées à leur ouverture complète (données dispersées, non agrégées et non homogènes, rupture de séries, niveau de granularité ou d'agrégation non pertinent) réduisent la fiabilité des données ainsi mises à disposition. Sur le plan financier, l'ouverture génère des coûts pour l'administration lorsqu'elle doit mettre à niveau ses données ou les mettre à jour régulièrement. L'équation budgétaire devient encore plus compliquée à résoudre lorsque l'opérateur, qui puise une partie de son financement dans la vente des données qu'il met à disposition des tiers [(2)], voit la redevance portant sur l'utilisation de ses données supprimée [(3)].

---

(1) Article 2 du décret n° 2014-1050 du 16 septembre 2014 instituant un administrateur général des données.

(2) Plusieurs opérateurs tirent une part non négligeable de leurs ressources des recettes générées par la redevance portant sur l'utilisation de leurs données, comme l'Institut géographique national (5,8 %), le Service de l'observation et des statistiques (5,3 %), le Service hydrographique de la marine (2,5 %) ou l'Institut national de la statistique et des études économiques (2,2 %).

(3) Voir le rapport d'information (n° 589, session ordinaire de 2013-2014), op. cit., *pp. 133-142.*

3. Instaurer un véritable « droit de savoir » à l'égard de l'ensemble des informations intéressant la vie publique et démocratique

Forte de ce constat, la Commission considère que notre législation n'a pas tiré toutes les conséquences de la révolution technologique de la dématérialisation et des modifications des conditions techniques de diffusion et de réutilisation des données publiques. Si, grâce au numérique, l'accès à l'information est devenu plus souple pour l'usager et moins onéreux pour l'administration, ce droit n'en demeure pas moins encore largement inadapté aux attentes et aux exigences formulées par la société en matière de transparence publique.

Dans ces conditions, la Commission estime indispensable de renforcer le cadre juridique applicable au droit à l'information en France, en procédant à sa consécration explicite dans notre droit (***a***) et en élargissant la liste des informations susceptibles d'être portées à la connaissance du public (***b***).

a. La nécessité d'instaurer un droit à l'information d'intérêt public

De prime abord, la Commission s'étonne que notre *corpus* juridique demeure aussi silencieux sur la question du droit à l'information publique. Absent de la Constitution du 4 octobre 1958 (1), ce droit n'a jamais été explicitement reconnu en France autrement que sous les formes inabouties du droit d'accès ponctuel, de la diffusion en ligne et du droit à réutilisation. Le Conseil Constitutionnel en a bien déduit implicitement l'existence à partir de la liberté d'expression et de communication protégée par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 mais au seul bénéfice du lecteur, de l'auditeur et du téléspectateur, en dégageant un objectif de valeur constitutionnelle de pluralisme des quotidiens d'information politique et générale, sans lequel la libre communication des pensées et des opinions ne serait pas effective (2), et un impératif d'honnêteté de l'information (3).

Or, pour la Commission, **le droit à l'information ne saurait être seulement conçu comme une liberté reconnue à ceux qui font profession d'informer sur les faits et d'exprimer des opinions** ou exercée par le seul prisme d'une presse d'investigation indépendante ; il devrait être plus généralement ouvert à l'ensemble des individus, quelle que soit leur qualité.

C'est du reste ce que prévoient de nombreuses dispositions internationales, comme la Déclaration universelle des droits de l'homme du 10 décembre 1948 (4),

---

(1) *La révision constitutionnelle de juillet 2008 s'est bornée à ajouter à la liste des règles qui doivent être impérativement fixées par le législateur «* la liberté, le pluralisme et l'indépendance des médias *» (deuxième alinéa de l'article 34 de la Constitution).*

(2) *Décision n° 84-181 DC du 11 octobre 1984,* Loi visant à limiter la concentration et à assurer la transparence financière et le pluralisme des entreprises de presse, *considérant 38.*

(3) *Décision n° 86-217 DC du 18 septembre 1986,* Loi relative à la liberté de communication, *considérant 11.*

(4) *Son article 19 prévoit que «* tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit ».

ou le Pacte international relatif aux droits civils et politiques du 16 décembre 1966 (1). En Europe, l'article 10.1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CESDH) du 4 novembre 1950 stipule que « *toute personne a droit à la liberté d'expression (...)* [qui] *comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière* ». De même, la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000 (2), à laquelle le traité de Lisbonne du 13 décembre 2007 (3) a donné force contraignante, comporte aussi un article 11 relatif à la liberté d'expression et d'information, qui implique « *la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières* », et un article 42 aux termes duquel « [t]*out citoyen de l'Union ainsi que toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre a un droit d'accès aux documents des institutions, organes et organismes de l'Union, quel que soit leur support* ».

La Commission est convaincue que le droit à l'information figure parmi les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques et que ces garanties ne peuvent plus, à l'ère numérique, consister dans un simple droit d'accès aux documents administratifs. Elle considère que, malgré la qualité indéniable de son travail, la CADA demeure prisonnière d'un cadre étroit et inadapté aux besoins d'une démocratie moderne. En dépit de la rapidité de ses décisions et de la conception libérale et extensive qu'elle a développée de ses missions, ses avis sont inégalement suivis, transformant la liberté d'accès aux documents administratifs en droit trop indirect et conditionnel.

Elle relève d'ailleurs que cette liberté a été fortuitement reconnue en 1978, dans un texte dont l'intitulé – « *portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal* » – montre qu'il ne s'agit pas de la proclamation solennelle d'un droit fondamental, à la différence d'autres démocraties qui disposent d'un cadre juridique plus solide, singulièrement la Suède, les États-Unis ou le Royaume-Uni (voir l'encadré ci-après). Le fonctionnement même de la CADA paraît en retrait par rapport à celui de ses homologues, en particulier l'*Information Commissioner's Office* britannique (ICO), chargé de veiller à l'application du *Freedom of Information Act*, qui est ouvert à la société civile et dont le président, M. Christopher Graham, est un ancien journaliste de la BBC.

---

(1) Son article 19.2 dispose que « toute personne a droit à la liberté d'expression; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix ».

(2) Charte européenne des droits fondamentaux de l'Union européenne du 7 décembre 2000 (2010/C 83/02).

(3) Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne (2007/C 306/01).

La liberté d'accès aux documents publics en droit comparé

En **Suède**, le droit d'accès aux documents administratifs a été reconnu dès **1776** et consacré dans la **loi constitutionnelle de 1974**. Ce pays dispose d'un des régimes juridiques les plus libéraux, rendant librement accessible un très large panel de documents administratifs, y compris la correspondance officielle du Premier ministre et reconnaissant aux fonctionnaires et agents publics la liberté d'expression qui leur permet de partager avec des tiers les informations dont ils disposent. L'enracinement de la tradition de la transparence publique est également confirmé par l'absence d'organisme chargé de veiller à la communication des documents administratifs, tout contentieux éventuel étant traité par l'*Ombudsman* du Parlement, sorte de médiateur institutionnel.

Aux **États-Unis**, le ***Freedom of Information Act* (FOIA) du 4 juillet 1966** règle la question de l'accès aux documents administratifs au niveau fédéral tandis que les États fédérés ont leur propre législation. En pratique, la plupart des documents administratifs font l'objet d'une publication automatique les rendant directement accessibles par les citoyens.

En **Espagne**, la **Constitution de 1978** et une **loi du 26 novembre 1992** ont reconnu aux citoyens un droit d'accès aux documents administratifs.

En **Italie**, le droit à l'information existe depuis une **loi du 7 août 1990**, aux termes de laquelle tout acte est communicable, même ceux d'ordre interne pris par une administration ou utilisés par elle. Ce droit concerne toutes les administrations centrales et locales et s'étend aux entreprises publiques et aux concessionnaires de service public.

Au **Royaume-Uni**, les conditions d'accès aux documents administratifs sont régies par le ***UK Freedom of Information Act* (UK FOI) de 2000** pour les documents détenus par les autorités publiques d'Angleterre, du Pays de Galles et d'Irlande du Nord (100 000 institutions sont concernées) – qui a remplacé le *Public Records Act* de 1958 ayant accordé aux citoyens un droit d'accès aux archives publiques après un délai de 50 ans – et le *Scotland Freedom of Information Act* de 2002 pour ceux détenus par les autorités publiques écossaises.

En **Allemagne**, la **loi fédérale sur la liberté d'information**, qui date **de 2006**, a mis un terme à la protection systématique par le secret professionnel des documents fédéraux sauf si une législation spécifique en disposait autrement, et plusieurs Länder ont adopté des législations comparables.

Source : Étude de droit comparé sur l'accès aux documents administratifs de juillet 2010, réalisée par les services de la CADA et disponible sur son site internet.

En définitive, préalablement aux améliorations susceptibles d'être apportées au cadre légal existant, sur lesquelles elle reviendra ultérieurement, la Commission recommande de **consacrer un véritable droit fondamental à l'information d'intérêt public**. Elle estime en effet que la révolution numérique doit être l'occasion d'**instituer un nouvel âge démocratique** fondé notamment sur une conception ambitieuse du droit à l'information, véritable **« droit de savoir »** (1), combinant le droit d'obtenir des institutions publiques les informations qu'elles détiennent (obligation de transparence) et le droit de prendre connaissance d'informations en principe secrètes ou interdites d'accès lorsqu'un intérêt légitime le justifie (obligation de révélation) (2).

---

(1) Edwy Plenel, Le droit de savoir, *Don Quichotte éditions, 2013.*

(2) Cour de cassation, Rapport annuel 2010 : Le droit de savoir, *pp. 63-290.*

En vertu de ce droit fondamental, **une présomption de libre communicabilité des documents d'intérêt public pourrait être instaurée**, à l'instar de ce qui se pratique aux États-Unis ou en Allemagne, obligeant l'administration à prouver la non-communicabilité d'un document et à justifier précisément sa décision. Cela permettrait de faire de la publicité des informations publiques un véritable principe et du secret une exception.

Un **service indépendant du droit à l'information**, bâti sur le modèle de l'ICO britannique, pourrait être chargé de mettre en œuvre ce nouveau droit en cas de conflit avec l'autorité publique détentrice d'une information, en se voyant reconnaître un champ de compétences élargi et des prérogatives renforcées par rapport aux pouvoirs aujourd'hui octroyés à la CADA. La Commission rappelle à cet égard que, à la différence de la CADA, certaines autorités administratives indépendantes françaises disposent de larges pouvoirs d'enquête et de sanction, comme l'Autorité des marchés financiers (AMF) ou la Commission nationale de l'informatique et des libertés (CNIL), même si aucune ne dispose du pouvoir de prescrire des mesures d'exécution de ses décisions à des personnes morales de droit public.

La Commission recommande d'examiner l'opportunité de **confier à l'autorité administrative indépendante chargée de veiller à l'application du droit à l'information davantage de pouvoirs décisionnels**, en lui confiant un pouvoir d'injonction sous astreinte visant à ce que l'administration récalcitrante publie les documents qui devraient l'être ou en lui donnant la faculté de saisir une juridiction lorsqu'elle observe un manquement à la législation. À l'étranger, si certains pays ont mis en place des entités indépendantes aux compétences exclusivement consultatives (Allemagne, Italie), d'autres leur ont confié des pouvoirs contraignants. C'est le cas au Royaume-Uni où l'*Information Commissioner* peut rendre des ordonnances exécutoires, précisant les actions à mener par l'administration, mentionnant, le cas échéant, des délais à respecter et indiquant les voies de recours ouvertes aux parties. Les ministres disposent, sous certaines conditions, d'un droit de veto face à de telles ordonnances, par exemple au cas où le document sollicité est classé confidentiel. En outre, l'*Information Commissioner* dispose d'un pouvoir de sanction.

Recommandation n° 1

Instaurer un droit fondamental à l'information d'intérêt public ouvert à tout individu et fondé sur une présomption de libre communicabilité des informations publiques.

Transformer les compétences et les prérogatives de l'actuelle Commission d'accès aux documents administratifs (CADA) pour en faire un service indépendant chargé de veiller à la bonne application de ce droit, doté de pouvoirs décisionnels, sur le modèle de l'*Information Commissioner* britannique.

b. Élargir la liste des documents communicables à l'ensemble des informations intéressant la vie publique et démocratique

Pour être effectif, ce nouveau droit à l'information doit **porter sur l'ensemble des informations qui intéressent la vie publique et démocratique**. De ce fait, il faudrait engager une réflexion approfondie sur les données qui doivent être communiquées et ouvertes, et faire appel à des concepts tels que les données d'intérêt général, ou les données de référence afin de créer un **service public de la donnée** exerçant une **mission de service public à part entière** pour assurer la transparence de l'action publique et permettre à la société française de tirer tout le parti des données numériques que l'État pourrait produire ou rendre accessibles.

La Commission considère qu'à l'ère numérique, marquée par la circulation rapide des informations et l'émergence de nouvelles exigences de transparence publique, la place prise par certaines de ces exceptions est devenue excessive. Les secrets et intérêts protégés par la loi, en particulier ceux concernant la sécurité nationale, la défense, la politique étrangère, la vie privée ou le secret industriel et commercial, ne sont d'ailleurs pas toujours compris par les citoyens et alimentent, souvent inutilement, la suspicion.

Il en va ainsi des exceptions liées au secret de la défense nationale, à la sûreté de l'État ou au secret des délibérations du Gouvernement. Comme l'a indiqué au cours de son audition du 9 juillet 2014 Mme Corinne Bouchoux, « *dans le domaine de la défense nationale, que le secret s'applique aux documents relatifs à la fabrication des bombes est tout à fait normal, mais il couvre aussi des informations qui devraient être publiques* ». Ainsi, la protection légitime de ces intérêts n'a pas empêché le service du renseignement allemand, le *Bundesnachrichtendienst* (BND), de décider de lui-même de rendre publics des documents relatifs à sa propre histoire. Aux États-Unis, les sites de l'administration américaine rendent en principe accessible l'ensemble des registres détenus par celle-ci, y compris ceux du Département de la défense et de la *National Security Agency*.

Le secret commercial et industriel, qui recouvre le secret des procédés, le secret des informations économiques et financières et le secret des stratégies commerciales, conduit lui aussi à restreindre l'accès à certaines informations techniques et financières figurant dans les documents mis à disposition dans le cadre des procédures de consultation publique. Mme Corinne Bouchoux s'est, à cet égard, interrogée à juste titre sur la notion de « vie privée d'entreprise » récemment dégagée par le Conseil d'État qui a jugé que « *la protection de la vie privée que l'article 6 de la loi du 17 juillet 1978 garantit à toute personne, tant physique que morale* » interdit « *de divulguer des choix révélateurs des actions et des projets d'entreprises de nature à porter atteinte au secret en matière commerciale et industrielle protégé par les mêmes dispositions* » [(1)].

---

(1) CE, 17 avril 2013, n° 344924.

Dans ces conditions, la Commission recommande que la liste des documents susceptibles de faire l'objet d'une publication soit sensiblement élargie en supprimant ou en assouplissant certaines des exceptions prévues par la loi n° 78-753 du 17 juillet 1978 précitée ou d'autres textes.

L'équilibre à trouver entre l'exercice du droit de savoir au nom de l'intérêt général et la préservation, lorsqu'elle est justifiée, de la confidentialité dépend de la nature des informations et des dommages éventuels qui pourraient résulter de leur communication. Il conviendrait désormais à l'ère numérique d'ériger le droit de savoir au rang de règle générale et de faire du secret l'exception, notamment dans certains cas portant sur les actions des pouvoirs publics ou les accords et partenariats qu'ils passent avec des acteurs privés, en confiant au juge le soin de trancher les différends en cas de refus de communiquer un document.

- *Les documents préparatoires*

S'il est normal que les documents inachevés ne soient pas communicables, tel ne devrait pas être le cas de certains avis ou documents préparatoires à une décision, même lorsque cette dernière est toujours en cours d'élaboration. Outre que cette catégorie recouvre un ensemble particulièrement vaste et hétérogène de documents, allant de l'avis d'un organisme à des rapports administratifs, les documents préparatoires sont souvent des éléments d'information qui méritent d'être connus et communiqués.

Il est à cet égard intéressant que le pouvoir exécutif ait décidé, le 20 janvier 2015, de rendre systématiquement publics les avis du Conseil d'État sur les projets de loi alors que, jusqu'à cette décision, seuls ceux pour lesquels il avait autorisé une telle publication pouvaient être diffusés et commentés dans le rapport annuel de cette juridiction. Aussi ces avis sont-ils, depuis le 19 mars 2015, rendus publics à l'issue du conseil des ministres qui en a délibéré [(1)], joints aux projets déposés au Parlement et diffusés dans les dossiers législatifs des projets de loi sur le site internet des assemblées. Il conviendra toutefois de traduire en droit cette nouvelle pratique.

En conséquence, la Commission recommande **de faire évoluer le cadre de communication des documents préparatoires tout en préservant les conditions nécessaires à une prise de décision sereine**.

Recommandation n° 2

Élargir la catégorie des documents communicables à certains documents préparatoires ou préalables à la décision d'une autorité publique.

(1) Ils peuvent notamment être consultés sur le site internet de Légifrance.

- *Les informations publiques comportant des données personnelles*

Le législateur pourrait, sans porter une atteinte excessive aux intérêts qui s'attachent à la protection de certains secrets, étendre les cas dans lesquels la publication d'informations publiques est nécessaire. Au Royaume-Uni, en application du *UK FOI*, qui a notamment permis de mettre au jour le scandale des notes de frais des parlementaires, les administrations sont tenues d'appliquer le **test de l'intérêt général** (*public interest test*) afin de déterminer s'il est dans l'intérêt public de maintenir confidentiel un document soumis à une exception de non-communicabilité.

Cela vaut en matière de protection de la vie privée. Comme l'a fort justement relevé M. Serge Daël au cours de son audition du 9 juillet 2014, « *si à chaque fois qu'une information peut être rapportée à une personne, on considère qu'elle ne peut être diffusée sans le consentement de l'intéressé, la vie démocratique et les débats publics ne sont plus possibles* ».

Toute donnée personnelle ne relève pas nécessairement et en toutes circonstances du domaine strictement privé qui, à l'ère numérique, a vu son périmètre et sa conception profondément évoluer [(1)]. La CADA, confortée par les décisions du juge administratif et en conformité avec la jurisprudence de la Cour européenne des droits de l'homme (CEDH), admet de longue date la communicabilité d'informations portant sur certaines données nominatives de personnes en raison des fonctions qu'elles exercent (hommes politiques, hauts fonctionnaires, etc.) et de l'intérêt public que ces informations représentent [(2)]. En Suède, un citoyen peut obtenir gratuitement et sans difficulté la copie de la fiche de paie d'un ministre ainsi que ses dépenses de représentation en se présentant directement auprès du ministère. La loi pourrait donc **préciser dans quelles conditions certaines informations personnelles d'intérêt public pourraient être publiées par l'administration**.

Recommandation n° 3

Moduler la confidentialité attachée aux informations à caractère personnel lorsqu'elles présentent un intérêt public important.

Par ailleurs, comment concilier spécifiquement la protection des données personnelles et l'exigence d'ouverture des données publiques ? Avec le *big data*, certaines données considérées comme anonymes peuvent constituer des données personnelles si elles permettent de réidentifier indirectement ou par recoupement

---

(1) Voir infra, *le III.*

(2) Sont ainsi communicables pour la CADA : l'arrêté de nomination d'un fonctionnaire (avis n° 20050537 du 3 février 2005), la liste des agents d'une commune (CE, 10 avril 1991, Commune de Louviers), la liste des enseignants par établissement (avis n° 20073195 du 13 septembre 2007), un organigramme des services d'une commune (avis n° 20060660 du 2 février 2006), les contrats de recrutement de chargés de mission d'un conseil général (avis n° 19950659 du 16 mars 1995), ou encore des décisions de nomination et de promotion des agents (avis n° 20000261 du 20 janvier 2000).

d'informations une personne. Le risque pour la protection des données personnelles ne dépend pas seulement de la sécurité offerte par la technique d'anonymisation [(1)], c'est-à-dire la confidentialité des outils de codage utilisés, mais aussi de la possibilité d'établir des liens entre les données anonymisées par recoupements ultérieurs, comme ce fut le cas pour certaines données ouvertes par de grandes entreprises américaines notamment (*AOL* [(2)], *Netflix* [(3)], etc.).

La Commission considère cependant qu'il ne faut pas surestimer les risques que présente l'*open data* pour la protection des données personnelles. La grande masse des jeux de données publiques mises en ligne par les administrations publiques porte sur des données non personnelles. De plus, la robustesse et la fiabilité des règles et des techniques d'anonymisation utilisées par les administrations publiques en présence de données personnelles réduisent considérablement l'importance des risques de violation de la vie privée. Ainsi n'y a-t-il eu qu'une seule faille de sécurité des données mises en *open data* par un opérateur public en France, lorsque l'Institut national de la statistique et des études économiques (INSEE) a publié, en 2013, une analyse sur l'imposition moyenne des habitants [(4)].

La Commission recommande d'**élaborer une doctrine, partagée par l'ensemble des opérateurs publics, afin d'anticiper et d'évaluer les risques pesant sur la protection des données personnelles qui résulteraient de l'ouverture des données publiques. Elle préconise d'adapter les formats de diffusion des données en conséquence et de surveiller régulièrement les jeux de données diffusées susceptibles d'être compromises**. À cette fin, et dans l'esprit des recommandations déjà formulées par d'autres, en particulier les sénateurs Gaëtan Gorce et François Pillet, rapporteurs d'une mission d'information sur l'*open data* et la protection de la vie privée (voir l'encadré ci-après), la Commission suggère de développer, en amont de leur ouverture, des **standards d'anonymisation** des données publiques et, en aval, une **licence spécifique de réutilisation des données anonymisées comportant plusieurs clauses restrictives et responsabilisantes** : obligation de préciser que les données ouvertes ont été anonymisées, interdiction de procéder à des recoupements ou tout

---

(1) Trois techniques d'anonymisation peuvent être utilisées : la pseudonymisation, qui consiste à remplacer l'identifiant initial par un autre identifiant arbitraire soit de manière réversible (table de correspondance secrète, algorithme de chiffrement), soit de manière irréversible (hachage simple, hachage avec clé secrète, double hachage avec clé secrète) ; le masquage, qui consiste à dégrader l'identifiant initial en en supprimant certaines données ou en ajoutant d'autres ; l'agrégation, d'usage courant en statistique, qui consiste à rassembler plusieurs données de même type afin de produire une donnée agrégée.

(2) En 2006, malgré l'anonymisation par pseudonymisation dont elles avaient fait l'objet, les données mises en ligne par AOL *sur les recherches effectuées sur son site par 650 000 utilisateurs ont permis d'identifier certains internautes qui vérifiaient régulièrement ce qui était publié à leur sujet ou réalisaient des recherches sur des services proches de chez eux.*

(3) Les informaticiens Arvind Narayanan et Vitaly Shmatikov sont parvenus à réidentifier certains utilisateurs du service de location en ligne de DVD de Netflix *dont les recommandations et notes avaient été publiées par l'entreprise après avoir été anonymisées.*

(4) Pour ce faire, l'INSEE avait découpé la France en carrés de 200 mètres de côté auxquels il avait associé un taux d'imposition moyenne : certains carrés étant situés sur des territoires faiblement peuplés ne comptant qu'un seul foyer fiscal, ils permettaient de remonter facilement à l'identité et à l'adresse de celui-ci.

autre pratique destinés à les rendre identifiantes, engagement de la responsabilité du réutilisateur, etc.

Les recommandations de la mission d'information sénatoriale sur l'*open data* et la protection de la vie privée [(1)]

– « *prévoir, dès la conception de la base, dans la perspective de sa possible réouverture (…) les modalités de son anonymisation éventuelle* » et du marquage des jeux de données aux fins de suivre leur réutilisation, et « *procéder à une analyse du risque de réidentification et des conséquences possibles d'une telle réidentification* » (recommandations n°s 5 et 6) ;

– « *en cas de risque avéré sur les données personnelles, impossible à éliminer par des procédés d'anonymisation* », renoncer à l'ouverture des données, procéder à leur ouverture partielle ou permettre d'autres modalités d'accès plus adaptées (recommandations n°s 7 et 8) ;

– « *assurer une veille sur la diffusion et les réutilisations des données publiques* [et] *(…) sur les données publiées par des tiers sur les sites publics* » et définir « *une stratégie de rapatriement ou de suppression des jeux de données compromis, afin de remédier rapidement à la diffusion accidentelle d'informations personnelles* » (recommandations n°s 9 à 11) ;

– renforcer la protection offerte par les licences de réutilisation en excluant de leur champ d'application les données personnelles, en « *interdi*[sant] *toute réutilisation abusive qui aboutirait à lever l'anonymisation des données* » et en « *intégr*[ant] *au contrat de licence, une clause de suspension légitime du droit de réutilisation, ainsi que de suppression ou de rapatriement des jeux de données compromis lorsqu'un risque de réidentification est apparu* » (recommandations n°s 12 à 14).

*(1) Rapport d'information (n° 469, session ordinaire de 2013-2014) de MM. Gaëtan Gorce et François Pillet au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur l'*open data *et la protection de la vie privée, avril 2014, pp. 60-66.*

Cette démarche pourrait également s'inspirer de la réflexion qui a été menée en matière d'ouverture des données publiques de santé, à la fois éléments de la vie privée des individus auxquels elles se rapportent et facteurs d'amélioration de la connaissance du secteur sanitaire, et dont la mise à disposition peut être conciliée avec la protection de certaines informations personnelles, grâce à la mise en place d'accès restreints aux données les plus sensibles (voir l'encadré ci-après).

Pour la Commission, cette doctrine de protection des données personnelles, garantie d'une large ouverture des données publiques respectueuse des droits fondamentaux de chacun, suppose d'aider techniquement, matériellement et financièrement les collectivités publiques à intégrer ces exigences dans leurs démarches. À cette fin, pourraient être mobilisés les « correspondants Informatique et libertés » (CIL) désignés au sein des administrations ainsi que les PRADA, habitués à traiter ce genre de question. De même, les mesures d'anonymisation parfois coûteuses mises en œuvre pour permettre l'ouverture des données publiques devraient être financées ou soutenues par l'État.

L'accès aux données publiques de santé

L'**accès aux données de santé** enregistrées dans le système national d'information inter-régimes de l'assurance maladie (**SNIIRAM**), qui contient tous les remboursements d'ordonnances médicales et, par conséquent, de nombreuses informations à caractère personnel, se fait selon des modalités différenciées en fonction de la nature de l'entité concernée : d'une part, un **accès permanent à la totalité de la base** (pour les organismes gestionnaires de l'assurance maladie et les agences publiques exerçant une mission de veille dans le domaine de la santé), **aux données agrégées et à un échantillon de bénéficiaires** seulement (pour les ministères compétents, les agences régionales de santé, certaines agences de santé, certains centres de recherche et certaines fédérations professionnelles ou de patients) ou **aux seules données agrégées de la base** (pour les fédérations professionnelles régionales et les associations membres des collectifs associatifs de patients) et, d'autre part, un **accès ponctuel, limité dans le temps, à une sous-base du SNIIRAM ou à une extraction des données** (à des fins de recherche).

Par un important **avis du 21 novembre 2013**, la **CADA** a autorisé la communication au collectif *Initiative Transparence Santé* d'extractions de données relatives à la consommation du médicament *Mediator* au motif que si ces données « *revêtent un caractère médical,* [elles] *ne constituent pas un extrait des données source de la base mais (…) correspondent, après traitement automatisé d'usage courant de ces données, à des informations anonymes et globales, par année et par département, ne permettant pas, compte tenu de leur niveau d'agrégation, l'identification, même indirecte, des patients ou des médecins concernés* » (1).

En septembre 2013, le **rapport de M. Pierre-Louis Bras** sur la gouvernance et l'utilisation des données de santé a formulé trois propositions visant à élargir l'accès du public au SNIIRAM et au programme de médicalisation des systèmes d'information (PMSI) :

– « ***distinguer*** *autant que possible* ***les lots de données clairement anonymes des lots de données indirectement nominatifs*** » et, après une expertise publique sur les risques de réidentification, ouvrir l'accès aux lots de données qui peuvent sans risques être communiqués ou rendus publics, sous le contrôle de la CNIL ;

– « ***ouvrir l'accès aux lots de données anonymes*** *en distinguant la publication (gratuite) et des extractions ou des tableaux de bord à façon (payants)* » ;

– « ***limiter l'accès aux données indirectement nominatives*** *du système d'information* » en fonction de la finalité d'intérêt public poursuivie, de la qualité du protocole utilisé, du besoin d'accéder aux données, de la sécurité des procédures suivies et de la qualité du demandeur.

(1) Avis n° 20134348 du 21 novembre 2013, Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS de Paris).

(2) Pierre-Louis Bras, La gouvernance et l'utilisation des données de santé, *septembre 2013, p. 7.*

Ces préconisations permettent, aux yeux de la Commission, de se prémunir contre une interprétation trop extensive des risques de réidentification en matière d'*open data*, qui empêcherait la diffusion et la réutilisation de nombreux documents d'intérêt public.

Recommandation n° 4

Mieux concilier l'exigence de protection de la vie privée avec l'impératif d'ouverture et de réutilisation des données publiques, y compris lorsque ces dernières sont susceptibles de se rapporter ultérieurement à une personne identifiée, en mettant en place une doctrine de protection des données personnelles limitant au maximum les risques de réidentification.

- *Les pièces communicables par les services publics industriels et commerciaux*

En outre, en matière de secret commercial et industriel, la Commission propose d'**élargir la catégorie des pièces communicables par les services publics industriels et commerciaux**.

Comme l'a souligné devant la Commission M. Serge Daël lors de son audition le 9 juillet 2014, « *quand ces services agissent selon le droit privé, c'est parce que l'on a voulu qu'ils soient traités comme des entreprises et, soumis à la concurrence, ils ne peuvent supporter des obligations que n'a pas le secteur privé. Il n'empêche qu'ils restent des services publics. Dans l'état actuel des choses, leurs documents sont divisés en trois grandes catégories : ceux qui traitent de l'organisation du service public sont considérés comme des documents administratifs ; ceux qui se rapportent aux relations avec les agents et avec les clients relèvent du droit privé – ce qui se discute pour le conducteur de la rame de métro, qui a affaire à des usagers ; ceux qui concernent des marchés publics sont communicables ou non en fonction de leur rapport plus ou moins étroit avec le service public* ».

Sans proposer l'ouverture de toute leur activité, la Commission recommande de **mieux définir l'équilibre entre la protection de leur activité de marché et le droit légitime des citoyens à la transparence du fonctionnement des services publics auquel ils contribuent, qu'ils soient administratifs ou industriels et commerciaux (transports, eau, déchets, énergie, etc.)**.

Recommandation n° 5

Afin de renforcer la transparence du fonctionnement des services publics, élargir la catégorie des documents communicables par les services publics industriels et commerciaux (transports, eau, déchets, énergie, etc.).

- *D'autres informations d'intérêt général*

Tous les documents relevant du droit à l'information publique ne sont pas, *stricto sensu*, publics, c'est-à-dire produits ou détenus par des opérateurs publics ;

ils n'en demeurent pas moins d'intérêt public. Tel est par exemple le cas des partenariats public-privé (PPP), contrats administratifs par lesquels la personne publique confie à un tiers, pour une période déterminée, une mission globale ayant pour objet la construction ou la transformation, l'entretien, la maintenance, l'exploitation ou la gestion d'ouvrages, d'équipements ou de biens immatériels nécessaires au service public ainsi que tout ou partie de leur financement. Alors même que leurs effets relèvent, à l'évidence, de l'action publique et de l'intérêt général, leur contenu se trouve souvent dans les offres des entreprises parties prenantes, ce qui restreint l'accès aux documents concernés.

C'est la raison pour laquelle la Commission souhaite que le champ des informations communicables inclue **les données qui, bien que non détenues par l'État, les collectivités territoriales et leurs établissements publics, comportent une forte dimension d'intérêt général**.

Seraient concernés **les documents et les données des entreprises et des organismes fournissant des services considérés comme essentiels ou bénéficiaires de subventions publiques**, comme dans le secteur des communications électroniques, du logement, du sport ou de la culture. Afin qu'elle ne constitue pas une charge excessive, la communicabilité de ces informations devrait être laissée à l'appréciation des entreprises et des organismes concernés.

La Commission constate d'ailleurs que la possibilité de définir une catégorie juridique des « données d'intérêt général », suggérée, dans le domaine spécifique des transports, par le Comité sur l'ouverture des données de transport présidé par M. Francis Jutand [(1)], est envisagée par Mme Axelle Lemaire, secrétaire d'État chargée du Numérique, ainsi qu'elle l'a indiqué lors du débat d'orientation pour la stratégie numérique de la France qui s'est tenu en janvier 2015 à l'Assemblée nationale [(2)] et lors de son audition par la Commission le 18 mars 2015.

À titre d'exemple, l'article 4 de la loi pour la croissance, l'activité et l'égalité des chances ouvre l'accès aux données des services réguliers de transport public de personnes et des services de mobilité (arrêts, horaires, tarifs, informations sur l'accessibilité et la disponibilité, incidents constatés, calculateurs d'itinéraires multimodaux) de façon libre, immédiate et gratuite, dans un format ouvert permettant leur réutilisation. Les services concernés pourraient remplir cette obligation par l'adoption de codes de conduite, de protocoles ou de lignes directrices rendus publics.

---

(1) Rapport du Comité présidé par M. Francis Jutand remis au secrétaire d'État chargé des transports, de la mer et de la pêche, Ouverture des données de transport, *mars 2015, pp. 17-18.*

(2) Voir le compte rendu de la première séance du mercredi 14 janvier 2015 publié au Journal officiel de la République française *du 15 janvier 2015.*

Recommandation n° 6

Encourager les entreprises et les organismes fournissant des services considérés comme essentiels ou bénéficiaires de subventions publiques (télécommunications, logement, sport, culture, etc.) à communiquer les documents et les données d'intérêt général qu'ils détiennent.

B. ORGANISER LE DROIT À L'INFORMATION PUBLIQUE À L'ÈRE NUMÉRIQUE

Des trois modalités d'exercice du droit à l'information, une seule fait l'objet, à ce jour, en droit français, d'une obligation à la charge des administrations publiques, consistant pour elles à communiquer au citoyen qui le demande le document administratif dont il souhaite avoir connaissance. Les autres modalités d'exercice de ce droit – la diffusion de l'information publique et l'ouverture des données publiques à des fins de réutilisation – sont laissées, à quelques exceptions près [(1)], à la libre appréciation des collectivités publiques, alors même qu'une possibilité de réutiliser les données diffusées en *open data* est ouverte à ceux qui le souhaitent.

Pour la Commission, l'absence d'ouverture complète des données publiques est le produit du télescopage entre notre tradition de transparence et de redevabilité publiques et le *web 2.0*. Cette tradition, qui remonte à 1789, incite l'administration à attendre la formulation d'une demande préalable pour agir et le citoyen à s'inscrire dans une démarche précontentieuse à son égard. Pour la Commission, l'*open data* aurait dû et devrait permettre de renverser cette situation et de passer d'un droit d'accès à l'information publique limité à un véritable droit à l'information publique, où le communicable d'aujourd'hui deviendrait directement consultable et réutilisable sur internet sans qu'il soit nécessaire de l'exiger de l'administration.

Force est donc de constater l'insuffisante mobilisation des technologies numériques dans la mise en œuvre du droit à l'information publique. Pourtant, la généralisation de la mise en ligne des informations publiques (**1**) et de l'ouverture des données publiques (**2**) permettrait de régler les obstacles qui existent actuellement à la communication individuelle et à la demande de certains documents et de parachever l'édifice construit à partir de 1978.

---

(1) Voir supra, *au* b *du 2 du A du présent I, l'article 106 de la loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République qui instaure une obligation de transparence des données des collectivités territoriales de plus de 3 500 habitants.*

1. Généraliser la mise en ligne des informations publiques, sauf lorsqu'elle est manifestement impossible ou trop coûteuse

Modalités parmi d'autres de la diffusion des informations publiques, la mise en ligne est une chance pour l'exercice du droit à l'information. « *Le droit à communication ne s'exer*[çant] *plus lorsque les documents font l'objet d'une diffusion publique* » (1), l'amélioration des conditions de mise en ligne des informations d'intérêt public serait de nature à mieux remplir l'obligation de communication des documents administratifs posée par la loi de 1978.

C'est pourquoi la Commission préconise de **généraliser la mise en ligne des informations d'intérêt public**, qui devrait primer sur le droit d'accès individuel et à la demande aux documents administratifs. Pareille généralisation, qui, en s'appliquant en tout premier lieu aux documents les plus fréquemment demandés, aurait le mérite de rompre avec la logique actuelle de traitement ponctuel des demandes à la fois lourde et coûteuse, devrait plus généralement porter sur l'ensemble des informations et documents d'intérêt général communicables, sur le modèle de ce qui existe déjà en matière environnementale.

Corrélativement, **la qualité des informations ainsi mises en ligne devrait être mieux assurée**, grâce à une mise à jour régulière de leur contenu et à une rationalisation de leur organisation. Le droit à l'information ne doit en effet pas seulement concerner un large spectre de documents mais doit aussi porter sur des **informations accessibles**, grâce à une présentation claire, uniforme et facile à trouver, **documentées**, ce qui exige leur mise à jour fréquente, **et intelligibles**, ce qui implique d'y associer des explications textuelles ou graphiques lorsqu'elles présentent un certain degré de complexité.

Recommandation n° 7

Prioritairement à leur communication sur demande et à titre individuel, généraliser la mise en ligne des documents et informations d'intérêt public dans des conditions en garantissant l'accessibilité, la mise à jour et l'intelligibilité.

La mise en ligne constitue également une solution intéressante pour améliorer la communication des documents d'intérêt public contenant des données à caractère personnel en permettant, à travers des espaces personnels sécurisés, leur mise en ligne personnalisée au seul bénéfice de l'intéressé sans qu'il en ait fait la demande. En effet, comme l'a souligné M. Serge Daël devant la Commission le 9 juillet 2014, « *nombre de ces cas pourront être réglés par la création d'espaces personnels dans les administrations. Chacun peut ainsi se créer un espace sur le site impôts.gouv.fr et y accéder sans avoir besoin de faire une demande, d'attendre un courriel d'acceptation* ».

---

(1) Quatrième alinéa de l'article 2 de la loi n° 78-753 du 17 juillet 1978 précitée.

L'**accès individuel « traditionnel »** demeurera mais de façon beaucoup plus limitée. La Commission recommande de **le réserver aux situations dans lesquelles la mise en ligne serait manifestement trop coûteuse ou les exigences en matière de protection des données personnelles incompatibles avec toute mise en ligne**. Le numérique peut là-aussi permettre de mieux accompagner les individus dans leurs démarches, notamment par la mise en ligne de guides pratiques et de modèles types de demandes d'accès ou l'insertion, sur la page d'accueil de chaque administration, d'un point d'accès visible et unique pour les demandes de communication.

Recommandation n° 8

Conserver un droit d'accès individuel « à la demande » pour les situations dans lesquelles la mise en ligne est impossible ou manifestement trop coûteuse et mieux accompagner l'individu dans ses démarches (élaboration de guides en ligne, création de points d'accueil des demandes de communication sur chaque site internet de l'administration).

2. Inscrire dans la loi le principe d'ouverture des données publiques à des fins de libre et gratuite réutilisation

Les individus ne doivent pas seulement pouvoir accéder à l'information publique ; ils doivent aussi pouvoir la relayer, l'échanger, l'utiliser à d'autres fins que celle pour laquelle elle a été publiée : tel est le défi posé par l'approfondissement de la démarche d'ouverture des données publiques qui doit devenir le principe par défaut (***a***) et permettre leur réutilisation réellement libre et gratuite (***b***).

a. Poser dans la loi le principe d'ouverture des données publiques

La question de l'ouverture des données publiques est régie par la directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, dite « PSI ». Cette directive prévoit que les documents et informations détenus par les organismes du secteur public sont rendus réutilisables par des tiers, à des fins commerciales ou non commerciales mais ne s'applique pas, notamment, aux « *documents dont la fourniture est une activité qui ne relève pas de la mission de service public dévolue aux organismes du secteur public concernés (…) ; (…) aux documents dont des tiers détiennent les droits de propriété intellectuelle ; (…) aux documents dont l'accès est exclu conformément aux règles d'accès en vigueur dans les États membres, y compris pour des motifs de protection de la sécurité nationale (c'est-à-dire sécurité de l'État), défense ou sécurité publique,* [de] *confidentialité des données statistiques,* [de] *confidentialité des informations commerciales (par exemple secret d'affaires, secret professionnel ou secret*

d'entreprise) » [1]. Elle laisse aux États le soin de fixer les règles pratiques d'ouverture des données publiques.

Afin de franchir une nouvelle étape dans ce domaine et de faire de l'*open data* un outil au service de l'exigence de transparence démocratique, la Commission recommande d'amplifier la quantité et d'améliorer la qualité des données publiques disponibles et rendues réutilisables par des tiers. Si, pour certains, « *une démarche raisonnée d'ouverture des données publiques* » [2] ou le « *renforce*[ment] *de la dynamique de mise en ligne progressive des données publiques* » doivent être privilégiés, la Commission estime pour sa part nécessaire d'**édicter un principe général d'ouverture des données publiques instaurant à la charge des administrations une obligation légale d'ouverture de leurs données** [3]. Ce principe d'ouverture des données publiques pourrait être inscrit dans la loi à l'occasion de la transposition prochaine de la directive dite « PSI ».

Pour la Commission, l'inscription d'un tel principe dans la loi est nécessaire pour au moins trois raisons :

– tout d'abord, même si le cadre incitatif et volontariste aujourd'hui mis en place par des instruments de droit souple a incontestablement permis à la France d'ouvrir sur la plateforme data.gouv.fr d'importantes bases de données publiques, une nouvelle étape doit être franchie en la matière pour renforcer la portée juridique de cette démarche et amplifier l'implication des collectivités publiques dans sa mise en œuvre ;

– par ailleurs, là où la démarche actuelle d'*open data* conduite par le Gouvernement s'adresse aux seules administrations de l'État et à ses opérateurs, l'instauration d'une obligation légale d'ouverture des données publiques permettrait d'y soumettre les autres collectivités publiques, singulièrement les collectivités territoriales, qui détiennent elles-aussi des informations d'intérêt général et qui sont aujourd'hui inégalement impliquées dans l'ouverture de leurs données, notamment à travers l'initiative territoire.data.gouv.fr ;

---

(1) 1) de l'article 1er de la directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public. Elle ne s'applique pas non plus « aux documents dont l'accès est limité conformément aux règles d'accès en vigueur dans les États membres, notamment dans les cas où les citoyens ou les entreprises doivent justifier d'un intérêt particulier pour obtenir l'accès aux documents ; (…) aux parties de documents ne comportant que des logos, des armoiries ou des insignes ; (…) aux documents dont l'accès est exclu ou limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par la loi comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel ; (…) aux documents détenus par des radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour l'accomplissement d'une mission de radiodiffusion de service public ; (…) aux documents détenus par des établissements d'enseignement et de recherche, y compris des organisations créées pour le transfert des résultats de la recherche, des écoles et des universités, à l'exception des bibliothèques universitaires, et (…) aux documents détenus par des établissements culturels autres que des bibliothèques, des musées et des archives ».

(2) Rapport d'information (n° 589, session ordinaire de 2013-2014) précité, pp. 164-174.

(3) CE, 29 avril 2002, n° 228830.

– enfin, aux termes de l'article 34 de la Constitution, il ressort de la compétence du législateur de fixer les règles concernant « *les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » : au nombre de celles-ci figure le droit d'accès aux documents administratifs [(1)], ainsi que l'a expressément reconnu le Conseil d'État en 2002. La mise en ligne et l'ouverture des données publiques, prolongements de ce droit, devraient donc, en toute logique, être également prévues par la loi.

La Commission n'ignore pas les difficultés techniques et financières qu'une telle obligation d'ouverture risque de soulever pour les administrations et les opérateurs concernés. Aussi, préalablement à l'instauration de cette obligation, **il convient de préparer et d'organiser l'ouverture généralisée des données publiques**.

La Commission recommande de procéder au recensement de l'ensemble des données susceptibles d'être ouvertes et à l'analyse de leur statut juridique au regard des exceptions à la réutilisation posées par la loi, de leurs caractéristiques techniques (format), de l'intérêt qu'elles présentent pour le public et des coûts éventuels liés à leur ouverture (en termes d'anonymisation, de transcription, de documentation, etc.) afin de prioriser leur mise en ligne.

Plus généralement, **la Commission souhaite que la culture de l'*open data* et de la donnée publique soit davantage intégrée au fonctionnement même de l'administration, par la formation et la sensibilisation des agents publics à ses problématiques et le développement, en interne, de compétences techniques élevées**. À cet égard, elle propose de généraliser la désignation, au sein de chaque administration, de référents ou chefs de projet *open data*, et de renforcer le rôle confié par le pouvoir réglementaire à l'administrateur général des données en inscrivant dans la loi son statut et ses fonctions.

Recommandation n° 9

Instaurer une obligation légale d'ouverture des données publiques. Afin de satisfaire dans les meilleures conditions à cette nouvelle obligation, préparer l'ouverture généralisée des données publiques et diffuser la culture de l'*open data* au sein des administrations concernées, en inscrivant notamment dans la loi le statut et les missions de l'administrateur général des données.

---

(1) Voir supra, *le* a *du 2 du A du présent I.*

b. Inscrire dans la loi le principe de réutilisation libre et gratuite des données publiques

Par ailleurs, la Commission préconise d'**introduire dans la loi le principe selon lequel la réutilisation des données publiques est libre et gratuite**, conformément aux engagements pris par l'État en la matière depuis plusieurs années.

La libre réutilisation n'est possible que si l'administration a recours à des **formats de bases de données libres et ouverts**. Cette exigence est d'ailleurs posée par la directive précitée « PSI » qui prévoit que « *les organismes du secteur public mettent leurs documents à disposition (...) dans un format ouvert et lisible par machine, en les accompagnant de leurs métadonnées. Tant le format que les métadonnées répondent, autant que possible, à des normes formelles ouvertes* » (1). Elle définit le format ouvert comme « *un format de fichier indépendant des plates-formes utilisées et mis à la disposition du public sans restriction empêchant la réutilisation des documents* » et le format lisible par machine comme « *un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d'un fait et sa structure interne* » (2).

C'est dans cette voie que se sont déjà engagées les administrations. L'État et ses établissements publics administratifs utilisent exclusivement, depuis novembre 2011, la Licence Ouverte (*Open Licence*), conçue par Étalab et qui autorise la reproduction, la redistribution, l'adaptation et l'exploitation commerciale des données sous réserve de l'obligation de faire expressément mention de la paternité de la donnée. D'autres administrations publiques utilisent la licence ODbL (*Open Database Licence*) qui permet de copier, de modifier et de faire un usage commercial des données sous la triple réserve de citer leur source, de redistribuer sous des conditions de partage identiques les modifications qui y sont apportées et de maintenir ouverte la base de données.

La Commission invite à anticiper le plus en amont possible l'ouverture des données afin que les personnes qui souhaitent y accéder et les réutiliser puissent le faire dans les meilleures conditions possibles. Comme elle aura l'occasion de le souligner lorsqu'elle abordera le rôle des technologies dans la préservation des droits au respect de la vie privée et à la protection des données personnelles (3), la Commission encourage la prise en compte de l'exigence d'ouverture des données publiques dès le stade de leur production ou de leur recueil. Pour ce faire, elle soutient les recommandations déjà formulées par d'autres organes tendant à la

---

(1) 5) de l'article 1er de la directive 2013/37/UE du 26 juin 2013 précitée.

(2) 2) du même article 1er.

(3) Voir infra, *le* a *du 3 du A du III.*

définition d'un « *cadre de normalisation technique et juridique contraignant* » [1] des données publiques, notamment :

– par la constitution d'un « *référentiel général de réutilisabilité* » [2] qui guiderait l'ensemble des administrations concernées dans leurs pratiques (modalités de documentation et de constitution des jeux de données, formats, conditions d'anonymisation, granularité, etc.) ;

– par la mise en place d'outils juridiques standardisés limitant le nombre de licences types de réutilisation et soumettant l'éventuelle intervention de tiers privés dans la création ou la gestion de bases de données aux exigences de l'*open data*.

Recommandation n° 10

Inscrire dans la loi le principe de la libre réutilisation des données publiques, grâce à l'utilisation de formats de bases de données et de licences de réutilisation ouverts.

S'agissant du **principe de gratuité**, il a été progressivement posé en France à partir de 1997, dans le but de défendre une conception exigeante de la société de l'information et de mettre en place un accès plus aisé à l'information publique [3]. Jamais toutefois il n'a été inscrit dans la loi, l'article 15 de la loi n° 78-753 du 17 juillet 1978 précitée prévoyant simplement que la réutilisation des données publiques « *peut donner lieu au versement de redevances* », ce qui implique que la gratuité devrait être la règle générale.

La gratuité ne doit pas empêcher un nombre précisément délimité d'organismes de recourir, à titre exceptionnel, à des redevances de réutilisation. Elle implique en revanche un **encadrement strict des redevances** qui doivent devenir l'exception – ce qui semble être de plus en plus le cas [4].

Le recours à des redevances de réutilisation est déjà relativement bien encadré par la loi [5]. D'une part, la redevance doit être calculée en fonction des coûts supportés par l'administration, notamment les coûts de collecte et de production, et inclure une « *rémunération raisonnable des investissements* » engagés pour la mise à disposition des informations, leur anonymisation ou la

---

(1) Rapport d'information (n° 589, session ordinaire de 2013-2014) précité, pp. 168-172.

(2) Avis n° 12 du Conseil national du numérique du 5 juin 2012 relatif à l'ouverture des données publiques (« Open data »), proposition n° 9, pp. 15-16.

(3) Discours d'Hourtin du Premier ministre du 25 août 1997 ; décret n° 2011-577 du 26 mai 2011 relatif à la réutilisation des informations publiques détenues par l'État et ses établissements administratifs ; circulaire du 26 mai 2011 relative à la création du portail unique des informations publiques de l'État « data.gouv.fr » par la mission « Etalab » et l'application des dispositions régissant le droit de réutilisation des informations publiques (NOR : PRMX1114652C) ; décision n° 32 du Comité interministériel pour la modernisation de l'action publique du 18 décembre 2012.

(4) Voir Mohammed Adnène Trojette, Rapport au Premier ministre. Ouverture des données publiques. Les exceptions au principe de gratuité sont-elles toutes légitimes ?, *juillet 2013.*

(5) Article 15 de la loi n° 78-753 du 17 juillet 1978 précitée.

rémunération des droits de propriété intellectuelle. D'autre part, elle ne doit pas être discriminatoire : elle doit être perçue dans le respect de l'égalité de traitement entre les réutilisateurs sauf si l'exercice d'une mission de service public rend nécessaire l'octroi d'un droit d'exclusivité. Elle doit enfin s'accompagner d'une licence type fixant les conditions de réutilisation [(1)].

Au fil de l'ouverture des données publiques, l'État a également défini une doctrine en matière d'exception au principe de gratuité. Celle-ci précise que la réutilisation des données produites dans le cadre de missions de service public ne peut pas donner lieu au paiement de redevances, sauf si elles correspondent aux coûts générés par la mise à disposition des données ou à la fourniture de services à valeur ajoutée. Lorsque des redevances sont instaurées dans le but de garantir l'anonymisation des informations, celles-ci doivent être réduites au maximum sans affaiblir la protection de la vie privée. Enfin, les opérateurs dont la mission est de produire des données et qui sont en partie financés par des redevances de réutilisation « *doivent rechercher des modèles économiques leur permettant de faire face à un paysage économique en profonde reconstitution* » [(2)].

La directive « PSI », qui n'impose pas la gratuité de l'ouverture des données publiques, précise que « *lorsque la réutilisation de documents est soumise à des redevances, lesdites redevances sont limitées aux coûts marginaux de reproduction, de mise à disposition et de diffusion* », ce qui revient souvent à la gratuité. Elle ne soumet pas à ce principe de tarification au coût marginal les « *organismes du secteur public qui sont tenus de générer des recettes destinées à couvrir une part substantielle des coûts liés à l'accomplissement de leurs missions de service public* » et les « *documents pour lesquels l'organisme (…) concerné est tenu de générer des recettes suffisantes pour couvrir une part substantielle des coûts afférents à leur collecte, à leur production, à leur reproduction et à leur diffusion* ». Sont également exemptés du principe de la tarification au coût marginal les bibliothèques, les musées et les archives. En toute hypothèse, « *le montant total des redevances* [doit être calculé] *en fonction de critères objectifs, transparents et vérifiables* » et « *le total des recettes desdits organismes provenant de la fourniture et des autorisations de réutilisation (…) ne* [doit pas] *dépasse*[r] *le coût de collecte, de production, de reproduction et de diffusion, tout en permettant un retour sur investissement raisonnable* ».

En définitive, la Commission estime que les modalités de fixation des redevances, lorsqu'elles sont absolument nécessaires, doivent se faire en toute transparence et en fonction de critères tenant compte du mode de financement de l'opérateur, des efforts engagés par ce dernier pour s'adapter au maximum à l'exigence de gratuité de l'ouverture des données publiques ou de l'importance des coûts générés par cette ouverture.

---

(1) Article 16 de la même loi.

(2) Décision n° 26 du Comité interministériel pour la modernisation de l'action publique du 18 décembre 2013.

La Commission n'ignore pas que la généralisation législative du principe de gratuité aura des conséquences budgétaires pour les administrations soumises à l'obligation d'*open data* et, tout spécialement, pour les opérateurs dont les ressources proviennent en partie de redevances de réutilisation. Il appartient toutefois à l'État de **garantir la viabilité financière de l'ouverture des données publiques, condition *sine qua non* du droit à l'information publique et, plus généralement, de l'indépendance et de la pérennité du secteur public par rapport aux acteurs privés ainsi que de la diffusion maximale des externalités positives liées à l'utilisation des données publiques au sein de la société**. Ainsi que le propose le rapport de M. Mohammed Adnène Trojette, consacré à l'ouverture des données publiques, les collectivités publiques pourraient, lorsque c'est absolument nécessaire, penser des modèles soutenables de financement de la production et de l'ouverture des données publiques, en mobilisant des financements coopératifs, en tirant profit des informations enrichies par ceux auxquels elles ont été gratuitement ouvertes ou en développant, à côté d'un accès « standard », un accès « enrichi » payant à certaines données publiques assorties de possibilités de traitements ou de services supplémentaires, sous réserve toutefois de maintenir, en parallèle, un accès gratuit aux données publiques brutes [(1)].

Compte tenu de l'importance qu'ont ces principes sur l'effectivité du droit à l'information, l'accès libre et gratuit aux données publiques à des fins de libre réutilisation constitue un **bien commun informationnel** qu'il convient de protéger et de promouvoir au regard des autres bénéfices, notamment culturels ou économiques, qui peuvent en être retirés par chaque individu et la société tout entière : renforcement de la transparence administrative et du contrôle de l'action publique, amélioration de l'accès aux contenus culturels numérisés libres de droit (écrits, sons, images, vidéos tombés dans le domaine public), instauration d'un écosystème innovant, développement de l'économie numérique, etc.

Recommandation n° 11

Inscrire dans la loi le principe selon lequel la réutilisation des données publiques s'opère à titre gratuit, sauf dans les cas, exceptionnels et dûment justifiés, pour lesquels l'établissement d'une redevance est nécessaire.

C. RENFORCER LA PROTECTION DES LANCEURS D'ALERTE

Accéder librement à l'information publique ne suffit pas ; encore faut-il que ceux qui ont connaissance d'informations d'intérêt public sensibles et maintenues cachées puissent donner ou lancer l'alerte et le faire en toute sécurité, afin d'éviter que le secret de ces informations ne couvre des faits ou des comportements pénalement répréhensibles ou moralement condamnables. Comme l'a fort justement affirmé M. William Bourdon, avocat et président fondateur de

---

(1) Voir les propositions visant à « garantir le principe de gratuité et *[à]* passer à des modèles économiques plus dynamiques *» in Mohammed Adnène Trojette,* op. cit., *pp. 83-98.*

l'association Sherpa, devant la Commission le 25 septembre 2014, « *quand un citoyen, face à une grave atteinte à l'intérêt général, se trouve dépourvu de tout instrument d'action autre que la transgression, il doit bénéficier d'une bienveillance* ».

La notion de « lanceurs d'alerte », relativement nouvelle en France, est bien connue des pays anglo-saxons où ils sont désignés *whistleblowers*. Le terme *whistleblowing* – littéralement « donner un coup de sifflet » – a été popularisé dans les années 1970 aux États-Unis par M. Ralph Nader (1) lors de ses campagnes de défense des droits des consommateurs. Il se rapporte aux personnes qui, ayant connaissance de faits dont elles supposent qu'ils sont constitutifs d'infractions ou de manquements à une règle, souhaitent, de bonne foi, les porter à la connaissance de tiers ou du public (employeurs, autorités judiciaires ou administratives, presse, etc.). Pour cela, il convient de les protéger par des mécanismes les soustrayant à d'éventuelles représailles.

À première vue, la protection des « lanceurs d'alerte » n'est pas un sujet proprement ou exclusivement numérique : l'idée de permettre un signalement des activités supposées illégales a préexisté à la révolution numérique. Toutefois, cette question a ressurgi récemment dans l'affaire Snowden et se pose, plus généralement, à chaque fois que sont examinées les conséquences de l'utilisation de telle ou telle technologie sur l'exercice des droits et libertés à l'ère numérique. La Commission aura l'occasion d'y revenir en examinant plus spécifiquement les moyens juridiques susceptibles d'être mis en œuvre pour faire cesser un manquement à la législation en matière de protection des données personnelles, qu'il soit le fait d'acteurs privés (2) ou d'autorités publiques (3).

La Commission souhaite ici insister sur l'intérêt qu'il y aurait à mieux protéger les « lanceurs d'alerte » pour le droit à l'information publique, en permettant la mise au jour de documents, de données ou d'informations que l'intérêt général commande de rendre publics mais qui demeurent, pour de multiples raisons, secrets. Aujourd'hui soumis à un cadre juridique segmenté et partiel (**1**), il apparaît nécessaire de leur appliquer un statut général plus complet et plus protecteur (**2**).

1. Un cadre juridique segmenté et partiel

Le droit français protège déjà les personnes qui souhaiteraient témoigner de faits et de situations qu'elles connaissent dans l'exercice de leurs fonctions et qui sont susceptibles de contrevenir à la législation (***a***) mais ne comporte pas de dispositif général et complet de protection des lanceurs d'alerte (***b***).

---

(1) Ralph Nader, Peter J. Petkas et Kate Blackwell, Whistle Blowing*, Bantam Press, 1972.*

(2) Voir infra*, le* c *du 3 du B du III.*

(3) Voir infra*, le 2 du C du même III.*

a. Des mécanismes de signalement et de protection de leurs auteurs…

De manière générale, en application de **l'article 40 du code de procédure pénale**, « [t]*oute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* ».

D'autres dispositions éparses ont également institué des **dispositifs de protection de nature civile ou administrative, spécifiques** à certaines matières, contre toute sanction ou mesure de rétorsion susceptible d'être prononcée à l'égard d'un agent du secteur privé ou du secteur public qui aurait dénoncé certains types de faits. Ainsi, plusieurs règles du droit du travail et de la fonction publique interdisent ou sanctionnent de nullité le licenciement ou le prononcé d'une sanction ou d'une mesure défavorable à une personne qui témoigne de faits dont elle a connaissance dans l'exercice de ses fonctions en matière de discriminations (1), de harcèlement sexuel (2) ou moral (3), de corruption (4) et de faits susceptibles de porter gravement atteinte à la santé ou à l'environnement (5).

Le législateur a, en 2013, généralisé la protection dont peuvent bénéficier les « lanceurs d'alerte » sur le modèle de ce qui existait déjà en matière de discrimination, de harcèlement, de corruption et d'atteintes à la santé ou à l'environnement. La **loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière** a créé deux nouvelles dispositions :

– la première, au sein du code du travail, qui prévoit qu'« *aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation en entreprise, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat, pour* ***avoir relaté ou témoigné, de bonne foi, de faits constitutifs d'un délit ou d'un crime*** *dont il aurait eu connaissance dans l'exercice de ses fonctions* » (6) ;

– la seconde, dans la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, qui prévoit, symétriquement, qu'« *aucune mesure concernant notamment le recrutement, la titularisation, la formation, la notation,*

---

(1) Article L. 1132-3 du code du travail et articles 6 et 6 bis *de loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.*

(2) Articles L. 1153-3 du même code et 6 ter *de la loi n° 83-634 du 13 juillet 1983 précitée.*

(3) Articles L. 1152-2 du même code et 6 quinquies *de la même loi.*

(4) Article L. 1161-1 du même code.

(5) Article L. 1351-1 du code de la santé publique.

(6) Premier alinéa de l'article L. 1132-3-3 du code du travail.

la discipline, la promotion, l'affectation et la mutation ne peut être prise à l'égard d'un fonctionnaire pour ***avoir relaté ou témoigné, de bonne foi, de faits constitutifs d'un délit ou d'un crime*** *dont il aurait eu connaissance dans l'exercice de ses fonctions* » [(1)].

Fait notable, en cas de litige, un renversement de la charge de la preuve est prévu, obligeant le défendeur à prouver que la sanction ou la mesure de rétorsion qu'il a prononcée à l'égard du « lanceur d'alerte » est « *justifiée par des éléments objectifs étrangers à la déclaration ou au témoignage de l'intéressé* » [(2)].

De manière quasi-concomitante, le législateur a institué, à l'article 25 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, une nouvelle protection spécifique des personnes qui dénoncent une situation de conflit d'intérêts, laquelle ne constitue pas forcément « *un délit ou (...) un crime* » mentionné par les dispositions générales du code du travail et du statut des fonctionnaires.

b. … mais aucun dispositif général de protection des lanceurs d'alerte

L'état du droit existant apparaît à la Commission insatisfaisant : selon M. William Bourdon, auditionné le 25 septembre 2014, ce sont en effet pas moins de « *cinq lois différentes* [qui] *encadrent la protection des lanceurs d'alerte, cet éparpillement brouillant la lisibilité et la visibilité de la règle* ». Ces législations éparses sont de surcroît incomplètes.

La procédure de signalement prévue par l'article 40 du code de procédure pénale, bien qu'ancienne [(3)], apparaît doublement cantonnée, *ratione personae*, car elle ne concerne que les autorités constituées, les officiers publics et les fonctionnaires et *ratione materiae*, car elle vise seulement les infractions de nature criminelle et délictuelle. En pratique, le recours à cette disposition est limité, en raison notamment de la prégnance des règles relatives au secret et à la discrétion professionnels et au principe hiérarchique. Au surplus, l'absence de signalement au procureur n'est assortie d'aucune sanction, en particulier pénale, même si l'agent public peut voir sa responsabilité pénale engagée pour complicité par abstention, en application de l'article 121-7 du code pénal, l'inaction de l'agent pouvant engager sa responsabilité et l'exposer à une sanction disciplinaire dans certaines hypothèses.

Pour le reste, le besoin qu'a eu le législateur d'instituer simultanément, en 2013, non seulement un dispositif « général » de protection des auteurs de signalements de faits constitutifs d'un délit ou d'un crime mais aussi une nouvelle disposition en matière de conflits d'intérêts, sans abroger les droits d'alerte spécifique existants, démontre les limites actuelles de notre droit.

---

(1) Premier alinéa de l'article article 6 ter *A de la loi n° 83-634 du 13 juillet 1983 précitée.*

(2) Troisième alinéa de l'article 6 ter *A précité et second alinéa de l'article L. 1132-3-3 précité.*

(3) Déjà présente sous le Directoire dans le code pénal de Brumaire an IV, cette disposition a été reprise à l'article 29 du code d'instruction criminelle puis à l'article 40 du code de procédure pénale.

Le code du travail et le statut général des fonctionnaires ne protègent en réalité que les personnes relatant ou témoignant de bonne foi de faits constitutifs d'un délit ou d'un crime, **à l'exclusion, d'une part, des infractions de nature contraventionnelle et, d'autre part, des situations conformes à la loi mais contraires à l'intérêt général, à l'éthique ou à la morale**.

Malgré les progrès importants faits par notre pays en la matière grâce à la nouvelle législation de 2013, le caractère segmenté et limité de la protection accordée aux « lanceurs d'alerte » tranche avec les recommandations constamment formulées par de nombreuses organisations internationales, associatives ou institutionnelles, visant à l'adoption de mesures de protection allant au-delà de la dénonciation d'actes illégaux et retenant une définition large des révélations susceptibles d'entrer dans le champ d'une alerte.

Par exemple, l'assemblée parlementaire du Conseil de l'Europe considère que « *la législation de protection des donneurs d'alerte doit avant toute chose offrir une alternative sûre au silence, tout en évitant de représenter pour des donneurs d'alerte potentiels un "bouclier en carton", piège qui leur donnerait une fausse impression de sécurité* » (1) ; elle invite donc les États à adopter une législation complète en la matière (voir l'encadré ci-après). De même, dans un rapport de 2009, *Transparency International*, après avoir dressé un panorama des textes applicables dans dix pays européens, recommande d'adopter « *une seule législation, explicite, complète et détaillée, pour la protection des lanceurs d'alerte* » (2).

Les recommandations du Conseil de l'Europe en matière de protection des lanceurs d'alerte (1)

Le Conseil de l'Europe estime qu'une protection complète des lanceurs d'alerte :

– inclut « *tous les avertissements de bonne foi à l'encontre de divers types d'actes illicites, y compris toutes les violations graves des droits de l'homme, qui affectent ou menacent la vie, la santé, la liberté et tout autre intérêt légitime des individus en tant que sujets de l'administration publique ou contribuables, ou en tant qu'actionnaires, employés ou clients de sociétés privées (...), y compris les membres des forces armées et des services de renseignements* » ;

– comporte des dispositions en droit du travail (protection contre les licenciements abusifs et les autres formes de représailles), en droit pénal et procédure pénale (protection contre des poursuites pénales pour diffamation, violation du secret commercial ou de secrets d'États ; protection des témoins) et en droit des médias (protection des sources des journalistes) ;

– prévoit « *des procédures internes (...) pour (...) que les dénonciations (...) fassent l'objet d'une véritable enquête* » et « *que l'identité du donneur d'alerte ne soit divulguée*

(1) *Résolution 1729 (2010) « Protection des "donneurs d'alerte", adoptée le 29 avril 2010 par l'assemblée parlementaire du Conseil de l'Europe.*

(2) *Transparency International*, Alternative to silence : whistleblower protection in 10 European countries, *2009, p. 4.*

qu'avec son consentement, ou si cela permet d'éviter des menaces graves et imminentes pour l'intérêt public » ;

– et, « [l]*orsqu'il n'existe pas de voies internes pour donner l'alerte, ou qu'elles ne fonctionnent pas correctement, voire qu'il ne serait pas raisonnable de s'attendre à ce qu'elles fonctionnent correctement étant donné la nature du problème dénoncé par le donneur d'alerte, il conviendrait de la même manière de protéger celui qui utilise des voies externes, y compris les médias* ».

(1) Résolution 1729 (2010) « Protection des "donneurs d'alerte" », adoptée le 29 avril 2010 par l'assemblée parlementaire du Conseil de l'Europe.

Ainsi que l'a indiqué au cours de son audition du 25 septembre 2014 M. William Bourdon, « *il faut* ***aller vers une loi unique instaurant un mécanisme de protection universel****, éventuellement décliné en dispositions particulières selon les secteurs* » et « ***étendre la protection à ceux qui dénoncent des atteintes graves à l'intérêt général*** ». « *Si elle fait un pas important en direction de cette universalité, la loi du 6 décembre 2013 ne protège les lanceurs d'alerte que lorsque ces derniers veulent révéler une situation qui s'apparente à un crime ou à un délit.* ***Il existe pourtant des violations de la morale des affaires ou de l'éthique plus graves que bien des délits*** ». Ainsi M. James Dunne, à l'origine des révélations sur les conditions dans lesquelles l'entreprise Qosmos aurait livré du matériel de surveillance au régime de Bachar el-Assad, « *ayant alerté sur quelque chose qui ne relève ni d'un crime ni d'un délit (…), cet homme ne bénéficie aujourd'hui d'aucune protection dans la loi française* ».

C'est enfin au terme d'un constat similaire que le législateur a ajouté, par la loi relative au renseignement, un nouvel article L. 861-3 au sein du code de la sécurité intérieure visant à protéger un agent des services de renseignement qui constaterait, à l'intérieur de son service, des « *faits susceptibles de constituer une violation manifeste* » des dispositions légales applicables aux activités de renseignement et à lui permettre d'en saisir la Commission nationale de contrôle des techniques de renseignement (CNCTR). Selon M. Jean-Jacques Urvoas, rapporteur du texte au nom de la commission des lois de l'Assemblée nationale qui en est à l'origine, cette disposition vise « *des comportements délictueux* [ou] *un usage inopportun ou a-légal des techniques de renseignement* » [(1)], ne recouvrant pas totalement les faits visés par les dispositions actuelles du code du travail et du statut général des fonctionnaires, dans un domaine au surplus couvert par le secret défense.

2. Créer un statut général protecteur des « lanceurs d'alerte »

La Commission est profondément attachée à la défense d'un droit de signalement éthique et citoyen, allant au-delà de la simple révélation d'infractions pénales. Elle recommande donc d'instituer un statut général des lanceurs d'alerte, valant pour la révélation de faits aussi bien pénalement répréhensibles que

(1) Voir le compte rendu intégral de la première séance du jeudi 16 avril 2015 publié au Journal officiel de la République française *du vendredi 17 avril 2015.*

manifestement contraires à l'intérêt général (***a***) et garantissant à leur auteur une protection effective (***b***).

a. Élargir le champ du « droit d'alerte » aux faits manifestement contraires à l'intérêt général

La Commission n'entend pas ici encourager la dénonciation ou la délation. Elle est bien consciente que les conditions d'exercice du droit à l'information publique ne sauraient instaurer un climat de suspicion généralisée.

En revanche, elle souhaite que le cadre juridique aujourd'hui applicable à la révélation de faits susceptibles de constituer un crime ou un délit prenne davantage en compte les situations dans lesquelles les faits dont a connaissance le lanceur d'alerte mériteraient de faire l'objet d'un signalement, alors même qu'ils ne seraient pas pénalement répréhensibles.

Dans ces conditions, elle recommande d'**élargir la définition aujourd'hui donnée des faits susceptibles d'être relatés par toute personne qui en a eu la connaissance sans qu'aucune mesure défavorable ne soit prononcée à son égard**. Cette définition devrait couvrir **:**

– non seulement les « ***faits constitutifs d'un délit ou d'un crime*** » ;

– mais aussi les **faits manifestement contraires à l'intérêt général ou faisant peser sur sa préservation une menace grave et réelle justifiant qu'ils soient portés à la connaissance de tiers**.

S'il retenait cette solution, le législateur devrait, pour la Commission, préciser la notion de « *faits manifestement contraires à l'intérêt général ou faisant peser sur sa préservation une menace grave et réelle* » afin de se prémunir contre d'éventuels signalements mal intentionnés et susceptibles de nuire à la réputation ou à l'activité des organismes ou entreprises concernés.

À cette occasion, le législateur pourrait utilement rationaliser l'ordonnancement des dispositions relatives aux droits de signalement – spécifiques et général – et homogénéiser leur rédaction.

Recommandation n° 12

Élargir le champ du « droit d'alerte » aux faits manifestement contraires à l'intérêt général ou qui font peser sur sa préservation une menace grave et réelle justifiant qu'ils soient portés à la connaissance du public.

Ainsi définis et circonscrits, les faits dont le lanceur d'alerte pourrait légitimement témoigner permettraient de couvrir les « zones grises » mal appréhendées par le droit ou situées hors du champ de la répression pénale tout en les limitant aux seules affaires intéressant la vie publique et démocratique. Il peut s'agir par exemple de la révélation de conflits d'intérêts hors du champ de la loi

relative à la transparence de la vie publique ou de la mise au jour de scandales industriels ou financiers.

La Commission souligne que deux garanties supplémentaires permettent, en droit français, de poursuivre tout abus dans l'exercice de ce droit de signalement. Il s'agit, d'une part, des dispositions du code pénal relatives à la dénonciation calomnieuse [(1)] et, d'autre part, de l'article 27 de la loi du 29 juillet 1881 sur la liberté de la presse, qui réprime « [l]*a publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler* ». Il pourrait même être envisagé qu'en cas de dénonciation calomnieuse ou de diffusion de fausses nouvelles, le fait de rechercher l'immunité de la loi protectrice des « lanceurs d'alerte » constitue une circonstance aggravante renforçant les peines applicables.

b. Garantir une protection effective aux « lanceurs d'alerte »

La Commission considère que la protection des « lanceurs d'alerte » contre toute mesure professionnelle défavorable telle qu'elle est prévue par les articles L. 1132-3-3 du code du travail et 6 *ter* A de la loi n° 83-634 du 13 juillet 1983 précitée constitue un acquis important de notre législation et doit être préservée. La définition particulièrement large qu'ils ont retenue d'une telle mesure – discrimination à l'embauche, au recrutement ou à la titularisation, sanction disciplinaire, licenciement, mesure discriminatoire dans la rémunération, l'intéressement, la formation, le reclassement, la promotion, la mutation, etc. – est le gage d'une réelle protection.

En complément, elle suggère de **doter une personnalité indépendante et impartiale de prérogatives destinées à garantir l'effectivité de cette protection** qui peut être mise à mal en présence de faits particulièrement sensibles, dont la révélation pourrait exposer son auteur à des menaces ou à des risques importants. La Commission formulera ultérieurement des propositions spécifiques en matière de signalement dans le champ particulier de la protection des données personnelles, qu'il est légitime de confier à la CNIL [(2)], et des activités de renseignement, qui doit ressortir de la compétence de la future CNCTR [(3)].

Sans préjudice de ces recommandations, elle propose de **permettre à l'autorité indépendante chargée de mettre en œuvre le droit à l'information** – qu'elle a précédemment appelée de ses vœux [(4)] – **d'être saisie par toute personne qui souhaiterait porter à la connaissance du public des faits particulièrement sensibles, susceptibles de constituer un crime ou un délit ou manifestement contraires à l'intérêt général**. Il est indispensable que cette

---

(1) Articles 226-10 à 226-12 du code pénal.

(2) Voir infra, *le* c *du 3 du B du III.*

(3) Voir infra, *le 2 du C du même III.*

(4) Voir supra, *le 3 du A du présent I.*

autorité soit saisie dans des conditions garantissant, au moins dans un premier temps, l'anonymat du « lanceur d'alerte » ainsi que sa totale sécurité, par exemple par la création d'un canal d'information sécurisé.

Cette autorité administrative indépendante, qui pourrait être la CADA reconfigurée et dotée de compétences et de pouvoirs élargis, pourrait, après un examen attentif de la situation, apprécier la protection qu'il convient de donner au « lanceur d'alerte » et les suites à donner aux faits dont elle a été saisie, soit en les transmettant aux autorités judiciaires compétentes s'ils sont constitutifs d'un crime ou d'un délit, soit en ordonnant à l'organisme responsable qu'ils soient rendus publics. Si les faits ont déjà été rendus publics, cette autorité indépendante pourrait garantir la protection du « lanceur d'alerte » dans l'attente qu'un juge statue sur la légalité des éventuelles sanctions disciplinaires ou professionnelles dont il aurait fait l'objet en représailles de son témoignage.

La Commission insiste tout particulièrement pour que l'autorité chargée de mettre en œuvre cette protection dispose d'une impartialité et d'une indépendance réelles et incontestables. En l'absence de telles garanties, elle suggère de confier cette mission au Défenseur des droits qui, aux termes de l'article 71-1 de la Constitution, « *veille au respect des droits et libertés par les administrations de l'État, les collectivités territoriales, les établissements publics, ainsi que par tout organisme investi d'une mission de service public, ou à l'égard duquel la loi organique lui attribue des compétences* ».

Recommandation n° 13

Instaurer un canal d'information sécurisé au profit des lanceurs d'alerte leur permettant de saisir une personnalité indépendante chargée de les protéger contre d'éventuelles menaces ou représailles.

Cette personnalité pourrait être l'autorité administrative indépendante chargée de mettre en œuvre le droit à l'information publique si elle dispose d'une indépendance incontestable et de pouvoirs suffisants ou, à défaut, le Défenseur des droits.

II. DÉFENDRE LA LIBERTÉ D'EXPRESSION À L'ÈRE NUMÉRIQUE

L'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 consacre « *la libre communication des pensées et des opinions* » comme « *un des droits les plus précieux de l'homme* » en reconnaissant la possibilité de lui imposer certaines limites : « *tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi* ».

Les textes internationaux ont par la suite consacré plus explicitement les deux dimensions de la liberté d'expression à savoir le droit de « ***recevoir et de communiquer des informations*** », et ce, « ***sans considération de frontière*** ».

Ainsi l'article 19 de la Déclaration universelle des droits de l'homme (DUDH) du 10 décembre 1948 dispose-t-il que « *tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit* ». Cette définition est reprise par l'article 19 du Pacte international relatif aux droits civils et politiques du 16 décembre 1966.

L'article 10 de la Convention de sauvegarde des droits de l'homme adoptée par le Conseil de l'Europe le 4 novembre 1950 dispose que « *toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir et de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence des autorités publiques et sans considération de frontière* ». Cette définition est reprise à l'article 11 de la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000.

En France, les conditions d'exercice de cette liberté (limites et garanties) ont été précisées par **la loi du 29 juillet 1881 sur la liberté de la presse** qui constitue le texte fondateur de la liberté d'expression dans notre pays. Contrairement à ce que son nom indique, ce texte ne se limite pas à la presse mais constitue le **droit commun** de **la liberté d'expression** qui s'applique aux propos tenus par **chaque citoyen** sur des écrits, des imprimés, dans la rue, dans des lieux ou réunions publics. Un **régime dérogatoire** a **été défini pour l'audiovisuel** par la loi du 30 septembre 1986 relative à la liberté de communication, justifié par l'utilisation par ce secteur d'une ressource publique rare, les fréquences hertziennes.

Le numérique n'a pas élargi le champ de la liberté d'expression mais a renforcé l'effectivité de ce droit, c'est-à-dire la capacité des individus à en jouir réellement. En effet, comme l'a reconnu le Conseil constitutionnel dans sa décision n° 2009-580 DC du 10 juin 2009, internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur liberté d'expression dans ses deux dimensions. À travers la messagerie électronique, les réseaux sociaux, les

sites de partage de contenus, les blogs, les plateformes de discussion, internet et la révolution du *web 2.0* ont particulièrement renforcé la capacité des citoyens à jouir de leur liberté d'expression **dans sa dimension « active »** et à contribuer à la diffusion de l'information et à la circulation et l'échange d'idées et d'opinions. On peut même affirmer qu'avec internet **ce droit, longtemps réservé aux individus ayant accès aux médias traditionnels (presse écrite, audiovisuel, éditeurs) a cessé d'être théorique pour l'essentiel de la société**.

Le régime juridique de la liberté d'expression sur internet a été pour l'essentiel fixé par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) qui a transposé la directive n° 2000-31 du 8 juin 2000 sur le commerce électronique. Il repose sur l'application aux éditeurs de services de la loi du 29 juillet 1881 sur la liberté de la presse. Quant aux hébergeurs, nouvelle catégorie d'acteurs propre à l'ère numérique, afin qu'ils ne soient pas amenés à exercer une surveillance généralisée et une censure des contenus de tiers qu'ils rendent accessibles, ils bénéficient par rapport aux éditeurs d'un régime de responsabilité civile et pénale atténuée à l'égard des contenus illégaux. Ce régime est donc garant de la liberté d'expression permise à chacun par la révolution du *web 2.0* mais aussi de la liberté d'entreprendre et d'innovation puisqu'un régime d'obligation trop lourd limiterait l'attractivité du statut et constituerait un obstacle à l'entrée de nouveaux acteurs.

Or, cet équilibre fait aujourd'hui l'objet **d'importantes remises en question dans l'objectif de faciliter la lutte contre les contenus illégaux**. L'étude annuelle du Conseil d'État 2014 résume ainsi la problématique de la liberté d'expression à l'ère numérique : « *l'essor d'internet ne change pas les limites pouvant être imposées à la liberté d'expression mais amène à s'interroger sur les instruments de la lutte contre les contenus outrepassant ses limites* » [(1)].

À cet égard et de manière générale, la Commission regrette la tendance des pouvoirs publics à aborder internet trop systématiquement comme un univers essentiellement dangereux et menaçant en négligeant sa dimension d'outil au service de la démocratie. Alors que la Commission avait souhaité inscrire ses réflexions dans une démarche positive en envisageant le numérique comme un levier d'accélération démocratique et d'approfondissement des droits et libertés, force est de constater que la teneur des débats politiques et l'actualité législative l'ont obligée à adopter une démarche largement défensive en ce qui concerne les libertés et en particulier la liberté d'expression. Notre pays aura d'ailleurs connu, pendant l'année d'existence de la Commission, la mobilisation populaire la plus importante de son histoire en faveur de la liberté d'expression à la suite des attentats de janvier 2015 et une régression particulièrement nette de la protection de cette liberté avec l'adoption de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme et l'annonce de plus amples remises en cause de la loi du 29 juillet 1881.

---

(1) Conseil d'État, op. cit., *p. 98.*

La Commission estime que les défis, réels, posés par la lutte contre les contenus illégaux sur internet ne doivent pas conduire à la mise en place progressive de réponses qui, sans être efficaces, entraîneraient une régression globale des libertés à l'âge numérique. Elle met en garde contre la tentation du législateur de remédier à des dysfonctionnements, en particulier les lenteurs de la justice, en touchant à des principes de droit.

La Commission constate en effet que l'objectif de lutte contre les contenus illégaux sur internet aboutit aujourd'hui à une multiplication de propositions et d'évolutions législatives (remise en cause de la loi du 29 juillet 1881, tendance au renforcement du rôle des acteurs privés ou des autorités publiques dans la lutte contre les contenus illégaux en contournant l'autorité judiciaire) qui sont porteuses d'une régression majeure en matière de protection des libertés à l'ère numérique.

La Commission rappelle que la technologie n'est pas libératrice en soi. Il n'est donc pas à exclure que la révolution numérique, qui est porteuse d'un accroissement de l'effectivité de la liberté d'expression, et partant d'une refondation démocratique sur une base beaucoup plus informée, délibérative et participative, s'accompagne finalement d'une régression de la liberté d'expression et de l'État de droit.

Face à ce risque, la Commission souhaite affirmer plusieurs principes simples : le respect de la neutralité technologique en matière de liberté d'expression (**A**) qui implique le respect de la loi du 29 juillet 1881 (**B**) ainsi que le principe du recours au juge (**C**) comme garantie fondamentale de la liberté d'expression.

A. AFFIRMER LE PRINCIPE DE NEUTRALITÉ TECHNOLOGIQUE

La Commission est attachée au principe de neutralité technologique, énoncé notamment par l'article 19 de la Déclaration universelle des droits de l'homme qui consacre la liberté de recevoir et de répandre les informations et les idées « *par quelque moyen d'expression que ce soit* ». Elle estime que l'univers numérique ne saurait en tant que tel faire l'objet d'un régime dérogatoire en matière de liberté d'expression et qu'il n'y a pas lieu de remettre en cause des garanties et principes juridiques anciens (**1**), de lui appliquer le régime de l'audiovisuel (**2**) ou de traiter différemment un propos en fonction du support sur lequel il est diffusé sans que cette différence de traitement soit précisément justifiée (**3**).

1. L'application de plein droit à internet de la loi du 29 juillet 1881

Internet n'est pas un espace de non-droit. Les limites de la liberté d'expression s'appliquent dans l'espace numérique comme ailleurs. Comme l'indique le Conseil d'État dans son étude annuelle 2014 [(1)], « *par lui-même*

(1) Conseil d'État, op. cit., *p. 13.*

internet ne remet en cause ni l'existence de ces limites ni leur tracé ». Si les limites de la liberté d'expression s'appliquent à internet, ses garanties doivent également s'appliquer dans les mêmes conditions.

C'est pourquoi la LCEN a logiquement étendu aux éditeurs de services de communication au public en ligne la loi du 29 juillet 1881 qui punit les abus de la liberté d'expression (notamment la diffamation, l'injure, la provocation aux crimes et délits, en particulier la provocation à la discrimination ou à la haine envers des personnes en raison de leur origine, de leur religion ou de leur orientation sexuelle, la négation de crimes contre l'humanité) tout en prévoyant des garanties procédurales adaptées à la nature particulière de ces infractions qui touchent à « *l'un des droits les plus précieux de l'homme* ».

L'application du régime de la loi sur la presse à internet est conforme au principe de neutralité technologique s'agissant du **régime de droit commun de la liberté d'expression**. Rappelons que la loi de 1881 sur la liberté de la presse constitue le **socle de la liberté d'expression dans notre pays**. Comme il a été indiqué précédemment, contrairement à ce que son nom indique, ce cadre protecteur ne se limite pas à la presse mais encadre la liberté de chaque citoyen de « *parler, écrire, imprimer* » et s'applique aux propos tenus **par chaque citoyen** sur des écrits, des imprimés, dans la rue, dans des lieux ou réunions publics. Rien ne justifiait donc que ce texte ne s'applique pas également sur internet. À cet égard, le titre de la loi sur la presse apparaît trop limitatif et entretient l'idée erronée selon laquelle le champ d'application de cette loi se limiterait à la presse.

Aujourd'hui, **les éditeurs de services et l'ensemble des producteurs de contenus sur internet sont donc soumis à un régime calqué sur celui de la presse** : ils ne sont soumis à **aucune obligation de déclaration préalable** ou d'autorisation ; les seules limites à leur liberté d'expression sont celles définies par le chapitre IV de la loi du 29 juillet 1881, ces infractions étant poursuivies et réprimées selon les conditions définies par le chapitre V de cette même loi ; ils doivent désigner un directeur de la publication ; un droit de réponse est prévu par la LCEN, qui transpose à internet le régime défini par l'article 13 de la loi du 29 juillet 1881 pour la presse. Dans le cadre de ce régime, **seul le juge peut réprimer les abus de la liberté d'expression**.

Recommandation n° 14

Afin de mettre fin à l'opinion répandue selon laquelle le champ de la loi de 1881 sur la liberté de la presse se limiterait à la presse, la renommer « loi sur la liberté d'expression ».

2. L'exclusion de plein droit d'internet du régime de l'audiovisuel

Alors que la proposition d'étendre à internet le cadre juridique de la régulation audiovisuelle est régulièrement avancée dans le débat public, il

convient de rappeler que l'exclusion d'internet du champ de la régulation des contenus audiovisuels est de plein droit.

L'audiovisuel fait l'objet d'une régulation sectorielle très spécifique et d'un **régime de liberté d'expression dérogatoire du droit commun** défini par la loi du 30 septembre 1986 relative à la liberté de communication. Rappelons que la régulation sectorielle se justifie dans des secteurs d'activité favorisant la formation de monopoles. **Le régime de l'audiovisuel est fondé à l'origine sur la rareté des fréquences hertziennes qu'utilisent les opérateurs audiovisuels pour émettre leurs programmes,** rareté qui favorise la formation de monopoles ou ne permet l'entrée que d'un faible nombre d'acteurs auxquels il convient d'imposer des obligations, notamment en matière de pluralisme. L'utilisation gratuite de fréquences appartenant au domaine public par les acteurs de l'audiovisuel justifie par ailleurs que leur soit imposé, en contrepartie, un certain nombre d'obligations d'intérêt général comme la participation au financement de la création. Ce cadre juridique particulier se caractérise par un régime d'autorisation et un pouvoir de contrôle des contenus confié à une autorité administrative indépendante disposant d'un pouvoir de sanction.

Exiger l'extension des principes de la régulation des contenus audiovisuels à internet relève du contresens, internet n'étant pas marqué par les spécificités du secteur audiovisuel, en particulier la rareté des acteurs et l'utilisation gratuite du domaine public hertzien. Cette proposition est pourtant fréquente et parfois défendue au nom de la neutralité technologique qui voudrait que des « contenus audiovisuels » soient soumis à la même régulation quel que soit le support.

Dans son rapport annuel 2013, le CSA rappelle ainsi qu'une première étape a été franchie avec la loi du 5 mars 2009 relative à l'audiovisuel public, qui a fait entrer les « services de médias audiovisuels à la demande » (SMAD) dans le périmètre de la régulation du Conseil. Il propose d'aller plus loin et de soumettre les « *services audiovisuels numériques* » entendus comme « *les services de communication au public par voie électronique mettant à disposition du public ou d'une catégorie de public des contenus audiovisuels ou sonores* » à des règles en matière de respect de la protection de l'enfance et de l'adolescence, de la dignité de la personne humaine, de l'interdiction de l'incitation à la haine ou à la violence pour des raisons de race, de sexe, de mœurs, de religion ou de nationalité. Le CSA serait chargé de fixer les règles auxquelles ces services sont assujettis. En cas de manquement à ces règles, il pourrait prononcer des sanctions à l'encontre de l'éditeur.

Auditionné par la Commission le 3 juillet 2014, M. Giuseppe di Martino, secrétaire général de *Dailymotion* et président de l'Association des services Internet communautaire (ASIC), s'est exprimé contre la proposition du CSA : « *rappelons que le rôle du CSA vient de l'attribution à des acteurs de ressources rares, à savoir les fréquences, en contrepartie du respect de certaines règles comme les quotas, le soutien à la production ou des obligations en matière de*

programmes. Or, sur internet, il n'y a pas de barrière à l'entrée et la ressource n'est pas rare : la régulation ne peut donc exister en contrepartie d'une quelconque autorisation ». Pour M. Patrick Eveno, professeur à l'Université Paris 1, spécialiste de l'histoire des médias, entendu par la Commission le 25 septembre 2014, « *le CSA est le régulateur du marché de l'audiovisuel – il délivre les autorisations de diffusion et attribue les fréquences. D'autre part, il tente de s'arroger deux domaines : la déontologie – qui n'est pas dans sa mission première, à savoir faire respecter l'honnêteté de l'information – et, surtout, Internet. Or je ne vois pas au nom de quoi il pourrait s'accaparer la régulation d'Internet, même si un grand nombre de chaînes de télévision et de radio ont un site. Les sites de presse et les* pure players *n'ont pas à dépendre de cette instance* ».

D'autres acteurs estiment que l'avènement du numérique rend le contrôle particulier exercé sur les contenus audiovisuels par le CSA en partie obsolète. En effet avec la numérisation de la plateforme hertzienne, les fréquences ne présentent plus le même degré de rareté et la place de la télévision hertzienne dans la consommation de médias s'est considérablement réduite. Selon M. Emmanuel Derieux, « ***on ne se heurte plus exactement aux mêmes contraintes techniques qui ont pu jusque-là justifier un régime juridique particulier des médias audiovisuels*** » (1). Certains revendiquent par conséquent un allégement de ce contrôle voire sa suppression. M. Patrick Eveno, lors de son audition du 25 septembre 2014, a rappelé que « *l'existence du CSA trouve son origine dans la pénurie de fréquences ; il fallait donc les répartir. Depuis l'émergence du numérique, cette pénurie n'existe plus et, à la limite, le CSA n'a plus de légitimité* ».

Dans son étude annuelle 2014, le Conseil d'État estime que deux des fondements théoriques de la régulation audiovisuelle, l'occupation du domaine public et la nécessité de réglementer des programmes « linéaires » ne peuvent être transposés aux services audiovisuels accessibles par internet. « *Le premier est tiré des règles générales de la domanialité publique qui permettent à la personne publique d'imposer des obligations d'intérêt général aux occupants et ne peuvent s'appliquer aux services audiovisuels diffusés par internet, lesquels ne passent pas par l'utilisation privative du domaine public hertzien. Le second fondement tient à ce qu'il est convenu d'appeler le caractère « linéaire » de services audiovisuels classiques. Des chaînes de télévision ou de radio diffusent un programme conçu à l'avance et l'utilisateur qui accède à ces chaînes n'a d'autre choix que de les regarder dans l'ordre proposé. Sur internet, l'utilisateur peut passer comme il le souhaite d'un site à un autre et dispose donc d'une plus grande liberté de choix. La réglementation de l'audiovisuel a été en partie conçue en raison de l'influence considérable que pouvait donner à l'éditeur d'une chaîne le fait que le même contenu soit vu par des millions de personnes au même moment (ce qui justifie l'expression anglaise de « mass media »). Cette question de l'influence ne se pose pas dans les mêmes termes sur internet* ». Le Conseil d'État en déduit que « *les motifs d'un encadrement de la liberté d'expression par les pouvoirs publics ne*

---

(1) Emmanuel Derieux, Droit des médias, *Dalloz, 2013.*

sont pas aussi forts sur internet que pour les services audiovisuels classiques, et [qu']*il est préférable de réserver au juge le prononcé de mesures restrictives de cette liberté* » (1).

La Commission rappelle surtout que le premier fondement théorique de la régulation audiovisuelle, à savoir la rareté des fréquences, laquelle limite le nombre des acteurs, est totalement absent de l'univers numérique. Par conséquent, elle estime que **rien ne justifie l'extension du régime dérogatoire extra-judiciaire d'encadrement de la liberté d'expression spécifique à l'audiovisuel à internet**.

Recommandation n° 15

Ne pas étendre à internet le régime dérogatoire extra-judiciaire d'encadrement de la liberté d'expression spécifique à l'audiovisuel.

En revanche, le développement de la consommation audiovisuelle sur internet, l'augmentation substantielle, permise par le numérique, du nombre d'acteurs présents sur la plateforme hertzienne et le recul de la place de la télévision hertzienne dans la consommation médiatique pourraient à terme conduire à une remise en cause du mode de régulation spécifique de la liberté d'expression applicable à l'audiovisuel.

S'agissant de l'avenir de la régulation audiovisuelle, la Commission estime qu'il convient de bien distinguer les enjeux du financement de la création à l'ère numérique de la question de la liberté d'expression. Si l'objectif d'étendre en les adaptant les principes de l'exception culturelle à de nouveaux acteurs de l'univers numérique peut se justifier, cela n'implique pas d'étendre par la même occasion l'encadrement de la liberté d'expression spécifique à l'écosystème fermé de l'audiovisuel.

3. La nécessité de justifier tout traitement différencié fondé sur la technologie

C'est sur la base de ce principe que le Gouvernement français défend l'application d'un même taux de TVA aux produits culturels quel que soit leur support et en particulier l'application du taux super réduit de TVA aux services de presse en ligne, rendue possible par la loi n° 2014-337 du 27 février 2014 harmonisant les taux de la TVA applicables à la presse imprimée et à la presse en ligne. De manière générale, la Commission recommande le respect de la neutralité technologique en matière d'aides à la presse.

---

(1) Conseil d'État, op. cit., *pp. 231-232.*

Recommandation n° 16

Faire respecter le principe de neutralité technologique dans la définition de la politique publique de soutien à la presse, ce qui implique en particulier de défendre l'application d'un même taux de TVA, quel que soit le support.

La Commission estime également que la neutralité technologique s'oppose à la **création de circonstances aggravantes lorsque des délits sont commis par internet**.

S'appuyant sur l'argument d'une « spécificité d'internet » et notamment de son effet « amplificateur » ou « démultiplicateur », plusieurs textes ont introduit une circonstance aggravante liée à la diffusion sur internet. Pour sa part, la Cour européenne des droits de l'homme (CEDH) a développé une jurisprudence assez abondante qui témoigne de sa volonté d'appliquer à internet les principes généraux qu'elle a définis en matière de liberté d'expression, tout en reconnaissant à plusieurs reprises l'existence d'une circonstance aggravante liée à la diffusion sur internet.

Dans une recommandation publiée le 29 septembre 2014 (1), la Commission s'est prononcée contre l'article 5 de la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, qui a transféré les délits d'apologie du terrorisme et de provocation au terrorisme hors de la loi de 1881 vers le code pénal en créant une circonstance aggravante lorsque les propos ont été communiqués « *au moyen d'un service de communication au public en ligne* ». Une position largement majoritaire s'est exprimée contre cette disposition qui traduit **une défiance de principe à l'égard d'internet**. La Commission attire l'attention sur la **nécessité de justifier tout traitement différencié fondé sur la technologie** et estime qu'un tel dispositif se heurte au principe d'égalité devant la loi pénale. Interrogé sur ce sujet, lors de son audition du 13 novembre 2014, M. Marc Robert, procureur général près la cour d'appel de Versailles, auteur du rapport *Protéger les internautes : rapport sur la cybercriminalité*, a également jugé « *dangereux d'associer une circonstance aggravante à un mode de communication ou d'expression* ».

La Commission considère qu'**internet ne doit pas être systématiquement envisagé de manière négative.** Faire, par principe, de l'utilisation ou de la consultation d'internet une circonstance aggravante revient à exprimer une position de défiance à l'égard d'une technologie dont on a tendance à oublier qu'elle constitue aussi un espace d'interaction, de collaboration et de partage. La Commission estime même que contrairement aux médias traditionnels, internet, **en permettant le débat et l'interactivité**, **offre une plus grande faculté de distanciation vis-à-vis des contenus et favorise l'émergence de mouvements**

---

(1) Voir la recommandation du 29 septembre 2014 sur plusieurs articles du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme.

de mobilisation citoyenne contre les contenus odieux. Par ailleurs, l'effet amplificateur d'internet par rapport à d'autres médias comme la télévision ou la radio n'est pas démontré.

Recommandation n° 17

Ne pas faire par principe de l'utilisation d'internet une circonstance aggravante.

La neutralité technologique s'oppose également à la remise en cause dans l'univers numérique de principes anciens, comme la possibilité de recourir au pseudonymat, là encore au nom de la nécessité de mieux sanctionner les propos hors la loi. Des responsables politiques et observateurs s'attaquent pourtant régulièrement à « l'anonymat » sur internet en répandant l'opinion, erronée, selon laquelle il s'accompagnerait d'une absence de responsabilité. Le 16 décembre 2013, M. François Hollande, qui recevait le Conseil représentatif des institutions juives (Crif) à l'Élysée, avait par exemple fait part de sa volonté de lutter contre « *la tranquillité de l'anonymat qui permet de dire des choses innommables sans être retrouvé* » sur internet.

La Commission rappelle que « l'anonymat » autorisé par l'article 6-III-2 de la LCEN est en réalité une possibilité de pseudonymat, qui n'exonère aucunement celui qui y a recours de sa responsabilité à l'égard des propos illégaux (diffamation, injure, appel à la haine, etc.). L'article 6-III-2 dispose en effet que les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public que le nom, la dénomination ou la raison sociale et l'adresse de leur hébergeur, sous réserve de lui avoir communiqué les éléments permettant de les identifier. Les hébergeurs sont assujettis au secret professionnel pour tout ce qui concerne la divulgation de ces éléments d'identification mais ce secret professionnel n'est pas opposable à l'autorité judiciaire. Le propriétaire d'un blog ou le titulaire d'un compte *Twitter*, par exemple, même s'il reste anonyme pour le grand public, est tenu de déclarer sa véritable identité à son hébergeur et d'assumer ses éventuelles infractions.

Auditionnée par la Commission le 3 juillet 2014, Mme Marie Mongin, vice-présidente de la 17e chambre du tribunal de grande instance (TGI) de Paris, a rappelé que le pseudonymat sur internet ne soulevait qu'une question d'ordre pratique que la LCEN permet de résoudre en autorisant l'autorité judiciaire à requérir certaines informations à caractère personnel pour poursuivre les auteurs. Interrogée sur ce point lors de l'audition du Conseil d'État, le 16 octobre 2014, Mme Maryvonne de Saint-Pulgent a rappelé qu'« ***on ne peut pas, au nom des difficultés à faire reconnaître son préjudice, instaurer ce qui serait inévitablement considéré comme une censure*** » et mis en garde contre la tentation de ***« remédier à des dysfonctionnements en touchant à des principes de droit*** ».

Au contraire, plus que jamais à l'ère numérique, le pseudonymat apparaît comme une condition indispensable à l'exercice de la liberté d'expression et du droit à l'information mais aussi à la protection de la vie privée. Comme l'indique derrière son pseudonyme, Maître Eolas, un avocat au barreau de Paris auteur d'un des blogs les plus lus de France, « *le pseudonymat est quelque chose de naturel sur les réseaux, et même une prudence élémentaire face à un support hypermnésique. Il est temps que l'on cesse de le trouver suspect, et cela commencera en cessant de le confondre avec l'anonymat* ». Mme Nathalie Kosciusko-Morizet, alors secrétaire d'État chargée de la prospective et du développement de l'économie numérique, dans une réponse écrite du 20 juillet 2010 au député André Wojciechowski sur sa proposition d'obliger les internautes à déclarer leur véritable identité, rappelait qu'une telle proposition « *serait à la fois inopportune et inefficace. Elle serait en effet inopportune car elle entrerait en conflit avec la liberté d'expression. Pour donner un exemple, un blogueur n'osera plus donner son avis sur la politique de son entreprise ou sur celle du gouvernement, surtout s'il est fonctionnaire. Rappelons à titre d'illustration le litige soumis fin mai au conseil des prud'hommes de Boulogne-Billancourt, par des salariés licenciés pour avoir médit de leur employeur dans un échange privé* ». Si le pseudonymat facilite certains abus, que le droit permet de réprimer en tant que tels, il permet aussi à chacun d'exprimer une opinion sans être inquiété ou sans mettre en péril sa situation professionnelle. Il permet d'échanger sur des forums, réseaux sociaux et autres plateformes tout en préservant sa vie privée. À cet égard, les associations de protection de l'enfance et la CNIL recommandent en particulier aux enfants et aux adolescents de ne pas utiliser leur vraie identité sur les réseaux sociaux.

Recommandation n° 18

Réaffirmer la possibilité de recourir au pseudonymat sur internet.

À l'heure du *big data* et du renforcement des outils de la surveillance, se pose plutôt la question du statut des techniques d'anonymisation de type *Tor* (et technologies liées) et de chiffrement des communications. Ce thème sera abordé dans la partie III du présent rapport consacrée aux enjeux de la protection de la vie privée et des données à caractère personnel à l'ère numérique [(1)].

B. PRÉSERVER LA LOI DU 29 JUILLET 1881 SUR LA PRESSE, PILIER DE LA DÉMOCRATIE, AUJOURD'HUI MENACÉE

Comme indiqué précédemment, la neutralité technologique implique l'application à l'univers numérique des règles et principes protecteurs de la liberté d'expression, en particulier les garanties procédurales définies par la loi de 1881 sur la liberté de la presse. Or, la Commission constate que la tradition juridique construite autour de l'imprimé fait aujourd'hui l'objet de remises en cause aussi injustifiées que dangereuses. En janvier 2014, en clôture du forum international

(1) Voir infra, *le* a *du 3 du III.*

sur la cybercriminalité, M. Manuel Valls, alors ministre de l'intérieur, estimait que le traitement de certains délits d'opinion (apologie du terrorisme, incitation à la haine raciale, propos racistes ou antisémites) devait pouvoir être repensé « *sans toucher aux grands équilibres de la loi sur la presse de 1881* : ***la question est posée aujourd'hui compte tenu de la force de frappe d'internet et son influence sur les citoyens de savoir si la répression de tels délits relève encore de cette législation*** ».

Comme l'a souligné Mme Marie Mongin, vice-présidente de la 17e chambre du TGI de Paris, auditionnée par la Commission le 3 juillet 2014, les règles de procédure particulières fixée par la loi de 1881 sont des règles protectrices de la liberté d'expression : « *or on s'aperçoit qu'internet conduit à modifier ce droit en portant atteinte à des principes anciens* ».

La Commission s'alarme du risque de remise en cause globale de la loi sur la liberté de la presse du 29 juillet 1881, qui, comme le rappelle la Commission nationale consultative de droits de l'homme (CNCDH) dans un avis sur la lutte contre les discours de haine sur internet du 12 février 2015, « *est, depuis le 19ème siècle, un pilier symbolique de la démocratie française et sa norme fondamentale de protection de la liberté d'expression* » (1). Cette remise en cause déjà engagée avec l'exclusion de l'apologie du terrorisme et de la provocation au terrorisme de la loi sur la presse (**1**) entraînerait une régression majeure de la liberté d'expression à l'ère numérique, comme l'illustre l'annonce d'un projet visant à basculer de nouveaux délits d'opinion hors de cette loi (**2**). Par ailleurs, la Commission appelle à se garder d'une conception de la liberté d'expression à deux vitesses (**3**).

1. L'exclusion de l'apologie du terrorisme et de la provocation au terrorisme hors de la loi sur la presse : un effet de brèche majeur

Dans sa recommandation du 29 septembre 2014 sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, la Commission s'est exprimée contre le transfert de deux délits d'opinion (l'apologie du terrorisme et la provocation au terrorisme) de la loi de 1881 vers le code pénal. La Commission a vu dans ces mesures une « *illustration de la remise en cause des libertés publiques à l'ère numérique* » et exprimé ses **inquiétudes quant au risque que ce précédent ouvre la voie à une remise en cause plus globale de ce texte** (2).

En dépit de cette recommandation, l'article 5 de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a sorti les délits de provocation à la commission d'actes terroristes et d'apologie du terrorisme de la loi de 1881 pour les inscrire dans un nouvel article 421-2-5 du code pénal.

---

(1) CNCDH, Avis sur la lutte contre les discours de haine sur internet, *12 février 2015, § 15.*

(2) Voir la recommandation du 29 septembre 2014 sur plusieurs articles du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme.

Le Gouvernement a largement justifié cette évolution « *par le rôle joué par internet comme vecteur de propagation des appels à la commission d'actes terroristes et de recrutement de terroristes* ». Aux termes de l'exposé des motifs du projet de loi, « *afin d'améliorer l'efficacité de la répression en ce domaine et* ***en considération du fait qu'il ne s'agit pas en l'espèce de réprimer des abus de la liberté d'expression mais de sanctionner des faits qui sont directement à l'origine des actes terroristes****, il convient de soumettre ces actes aux règles de procédure de droit commun et à certaines règles prévues en matière de terrorisme (…)* ». L'insertion de ces délits dans le code pénal permet en effet d'appliquer les règles de procédure et de poursuites de droit commun, exclues en matière de presse, comme l'application d'un délai de prescription de trois ans, la possibilité de saisies ou la possibilité de recourir à la procédure de comparution immédiate.

La Commission récuse formellement l'argumentaire du Gouvernement selon lequel ces délits ne constitueraient pas des abus de la liberté d'expression mais « *des faits directement à l'origine des actes terroristes* ». On ne saurait affirmer qu'une opinion mène nécessairement à un acte et la loi de 1881 est précisément là pour distinguer ce qui relève de l'expression délictueuse de ce qui relève de l'acte délictueux. La Commission estime que la dissidence et l'appel à un renversement de l'ordre établi peuvent relever dans certains cas de l'opinion, et doivent donc être appréhendés dans le cadre d'une loi et de procédures spécifiques. Elle considère que l'apologie du terrorisme et la provocation à la commission d'actes terroristes constituent toujours, sur internet comme ailleurs, des abus de la liberté d'expression qui, en tant que tels, doivent continuer à être réprimés dans le cadre des procédures particulières prévues par la loi sur la liberté de la presse. Elle **récuse fermement l'idée selon laquelle internet modifierait la nature d'une infraction**.

L'argumentaire du Gouvernement a été contredit de manière frappante par la salve de condamnations totalement disproportionnées [(1)] **prononcées en application de ces nouvelles dispositions au lendemain des attentats de janvier 2015, pour des propos dont on ne saurait affirmer qu'ils sont « *des faits directement à l'origine des actes terroristes* »** [(2)]. De nombreux observateurs et plusieurs organisations telles que la Ligue des droits de l'homme et Amnesty international ont dénoncé des atteintes graves à la liberté d'expression, une « justice d'exception », « expéditive », menant à des peines trop lourdes. Comme l'a souligné Mme Christine Lazerges, présidente de la CNCDH, auditionnée par la Commission le 15 avril 2015, « *des centaines de majeurs et de mineurs ont été condamnés en comparution immédiate parce qu'ils avaient prononcé des mots certainement condamnables, mais pas tous forcément pénalement condamnables. Les poursuites et le comportement des magistrats, sous le coup de l'émotion suscitée par les attentats, immédiatement après l'adoption de la loi renforçant la lutte contre le terrorisme, nous ont convaincus*

---

(1) C'est ainsi que les a notamment jugées Pascal Beauvais, rapporteur de l'avis de la CNCDH sur la lutte contre les discours de haine sur internet, audition du 15 avril 2015.

(2) http://tempsreel.nouvelobs.com/charlie-hebdo/20150120.OBS0370/apologie-du-terrorisme-une-longue-liste-de-condamnations.html.

que nous ne nous trompions pas : pour des paroles, il faut rester dans le cadre de la loi de juillet 1881 ».

L'exclusion de ces délits hors de la loi sur la presse a constitué un effet de brèche majeur et rendu le droit illisible et incohérent. En effet, comment justifier que l'apologie du terrorisme soit réprimée plus durement que l'apologie de crime contre l'humanité, l'incitation à la haine raciale, antisémite, homophobe, sexiste etc. ? Dès lors que l'on accorde sans justification théorique valable un traitement particulier à certains délits d'opinion jugés particulièrement inacceptables en réaction à certains événements, la tentation est grande de multiplier ces exceptions jusqu'à en faire la règle. Force est de constater que les craintes de la Commission ont été confirmées par l'annonce dès janvier 2015 d'un projet de loi visant à basculer d'autres infractions hors du champ de la loi sur la presse.

Recommandation n° 19

Réintroduire le délit l'apologie du terrorisme parmi les infractions relevant de la loi de 1881 sur la liberté de la presse.

2. L'annonce d'un projet visant à basculer de nouveaux délits d'opinion hors de la loi sur la presse : vers la fin de la loi sur la presse ?

Dès le 16 janvier 2015, dans un communiqué de presse, la garde des Sceaux a ainsi annoncé sa volonté de sortir les injures et diffamations de la loi du 29 juillet 1881 pour les introduire dans le code pénal lorsqu'elles sont aggravées par une circonstance liée au racisme, à l'antisémitisme, à l'homophobie. Pour les raisons énoncées précédemment s'agissant de l'apologie du terrorisme, la Commission s'oppose fermement à cette évolution qui marquerait une profonde régression de notre droit fondamental.

La Commission estime, comme la CNCDH, que le mouvement de sortie de la loi du 29 juillet 1881 d'un certain nombre d'infractions relatives à la liberté d'expression vide cette grande loi de sa substance et lui fait perdre sa cohérence, au risque de la marginaliser et de la voir disparaître à terme.

Elle souhaite rappeler, comme le fait régulièrement la Cour de Strasbourg (1), que la liberté d'expression constitue l'un des fondements essentiels d'une société démocratique. Ce droit « *vaut non seulement pour les informations ou idées accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'État ou une fraction quelconque de la population. Ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de société démocratique* » (2). Ainsi la Commission est-elle, comme la CNCDH, « *fondamentalement préoccupée par la sauvegarde, et au besoin par l'extension,*

---

(1) Voir notamment CEDH, 7 décembre 1976, Handyside c. Royaume-Uni, *n° 5493/72 ; CEDH, 28 juin 2012,* Ressiot et autres c. France, *n°s 15054/07 et 15066/07.*

(2) CEDH, 7 décembre 1976, Handyside c. Royaume-Uni, *§ 49.*

de l'espace public de libre discussion qui est consubstantiel à la démocratie et à l'État de droit. L'impertinence, l'irrévérence, les idées qui dérangent sont une richesse inestimable pour l'éveil des consciences. Elles ont toute leur place dans l'espace public qui ne saurait être aseptisé par une domestication de la prise de parole » [(1)].

En outre, la Commission estime que l'on combat plus efficacement des propos et idées particulièrement odieux par le débat contradictoire qu'en interdisant leur expression.

La loi du 29 juillet 1881 définit de manière subtile et évolutive l'équilibre à maintenir entre la liberté d'expression qu'elle protège et ses limites. Comme l'a indiqué M. Pascal Beauvais, rapporteur de l'avis de la CNCDH sur la lutte contre les discours de haine sur internet entendu par la Commission le 15 avril 2015, « *ce grand texte libéral historique, socle de notre démocratie et qui a fait ses preuves, doit rester notre référence, notre texte fondamental en la matière. Les infractions qu'il contient, incriminant les abus de la liberté d'expression, doivent rester les mêmes ; il ne faut ni les élargir, ni en créer de nouvelles, ni aggraver les peines encourues. La loi de 1881 ne doit pas être détricotée : il ne faut pas en extraire certaines infractions pour les noyer dans le droit commun du code pénal. Elle doit conserver le monopole des infractions incriminant les abus de l'expression.*

« *Doit rester gravé dans le marbre de la loi le fait que les infractions incriminant les abus de l'expression et de l'opinion ne sont pas des infractions comme les autres. Potentiellement liberticides et anti-démocratiques, elles ne peuvent être qu'une exception très encadrée au principe général de liberté d'expression. Elles doivent donc être contenues dans une loi spéciale qui protège la liberté d'expression et qui offre des garanties et une protection elles aussi spéciales à celui qui s'exprime. Cette protection n'existe pas dans le code pénal. Dans la loi de 1881, celui qui s'exprime est protégé par une procédure d'offre de preuve et par la prise en compte du sérieux de son propos et de sa bonne foi. Il ne peut être l'objet de la procédure pénale expéditive entre les mains du Parquet et de la police que permettent par exemple la comparution immédiate ou la comparution sur reconnaissance préalable de culpabilité. Il est protégé des procédures abusives et éventuellement instrumentalisées par des délais de prescription réduits*.

« *Dans l'esprit du juge qui applique cette loi doit demeurer ce balancement : le principe est la liberté d'expression, l'exception, très strictement encadrée, étant l'abus de cette liberté. Le juge doit conserver la main tremblante de celui qui pose une limite à une liberté constitutionnelle en précisant dans sa jurisprudence les limites de la liberté d'expression. Le code pénal, orienté vers la répression des atteintes à l'ordre public, ne contient pas cette affirmation solennelle de la liberté d'expression. Il banaliserait ces infractions en les noyant dans les autres. La preuve en a été apportée, au lendemain des attentats de*

---

(1) CNCDH, op. cit., *§ 5.*

janvier 2015, par une salve de condamnations en comparution immédiate pour apologie du terrorisme totalement disproportionnées ».

Recommandation n° 20

Mettre un terme au transfert dans le code pénal des infractions à la liberté d'expression relevant de la loi de 1881sur laliberté de la presse.

3. Se garder d'une conception de la liberté d'expression à deux vitesses

La Commission constate l'émergence dans le débat public de l'idée selon laquelle pourraient se mettre en place des régimes différenciés de liberté d'expression en fonction de celui qui l'exerce, les journalistes professionnels bénéficiant d'un régime de liberté d'expression plus favorable.

Cette conception a notamment été défendue par Mme Axelle Lemaire, secrétaire d'État chargée du Numérique, qui, lors de son audition du 18 mars 2015, a évoqué l'idée de réserver l'application de la loi sur la presse aux seuls journalistes professionnels. « *S'agissant de la loi de 1881, (...) le diagnostic est largement partagé : cette loi formidable, écrite en 1881, s'appliquait à des situations qui ne connaissaient pas la massification de l'information. Aujourd'hui nous faisons face à un phénomène qui n'a pas été envisagé à l'époque : n'importe quel particulier, dans n'importe quel contexte, est susceptible de poster une information sur un réseau social, qui peut ensuite être démultipliée. En même temps, les victimes de propos haineux, racistes et antisémites exprimés sur internet – sur certains blogs, sites ou réseaux sociaux – font part d'un immense sentiment d'impunité. L'arsenal législatif pour réprimer ces délits existe, mais les procédures sont tellement complexes, difficiles d'accès et lentes qu'elles se révèlent inaccessibles au citoyen lambda qui se retrouve mal protégé contre ces dérives. Certes, la loi de 1881 bénéficie d'un socle jurisprudentiel important, des générations d'avocats et de magistrats spécialisés ayant parfaitement ajusté les équilibres entre la sécurité de nos concitoyens, le respect de la règle et celui de la liberté d'expression. Ces équilibres doivent être maintenus, mais* ***la loi sur la presse doit être*** *refondue et* ***actualisée à l'heure d'internet****. Il faut sans doute* ***distinguer deux statuts : celui des journalistes,*** *à protéger – l'objet initial de cette loi sur la presse* ***– et celui des internautes,*** *producteurs ou victimes, qui ne relèvent pas de l'information professionnelle ; en l'état, le texte n'opère pas cette distinction* ».

La Commission s'oppose fermement à cette conception d'une liberté d'expression à deux vitesses en décalage total avec la réalité d'un espace qui remet en cause les frontières du journalisme et où l'internaute, expert ou simple citoyen informateur, est devenu grâce aux outils mis à sa disposition un acteur privilégié de la communication, participant à la construction d'une intelligence collective, aux côtés des journalistes professionnels. Comme l'indiquait

M. François Ewald dans un article intitulé « Internet, la fin du journalisme » [1] « *les journalistes et les journaux d'opinion n'existeront peut-être bientôt plus, en tout cas au sens où nous les connaissons aujourd'hui. Avec Internet et les moteurs de recherche, l'information ne se fait plus du haut vers le bas, d'une élite journalistique vers un peuple dépendant et assoiffé d'une information rare et contrôlée, mais dans une capacité infinie de communication latérale de chacun avec tous. La grande révolution de la démocratie en cours est que le citoyen trouve avec Internet l'espace et le moyen d'une liberté d'expression affranchie de tout pouvoir – y compris de ce pouvoir de la Presse – censé l'affranchir de tous les pouvoirs* ».

Il convient de rappeler que les textes constitutionnels et conventionnels qui garantissent la liberté d'expression placent l'ensemble des citoyens à égalité devant cette liberté. La Commission estime que la création de deux régimes de liberté distincts ne saurait se fonder sur des différences suffisantes dans les conditions d'exercice de cette liberté alors que les internautes et blogueurs non professionnels participent aujourd'hui au moins autant que les journalistes à la vitalité du débat démocratique et à l'information publique.

Recommandation n° 21

Ne pas « réserver » les principes protecteurs de la liberté d'expression aux journalistes professionnels.

C. CONFORTER LA PLACE DU JUGE COMME GARANT DE LA LIBERTÉ D'EXPRESSION

Le régime de la liberté d'expression repose traditionnellement sur deux principes forts : l'absence de contrôle *a priori* des contenus et le principe selon lequel seul le juge peut apprécier ce qui excède l'exercice de cette liberté et prononcer des mesures restrictives de cette liberté.

La LCEN s'est attachée à préserver ces principes à l'ère numérique en soumettant les éditeurs de services sur internet à un régime calqué sur celui de la presse et en limitant le rôle des intermédiaires privés, en particulier les hébergeurs, dans la lutte contre les contenus illégaux.

Ces principes apparaissent aujourd'hui fortement remis en cause ou menacés par de très nombreuses propositions dont le dénominateur commun est de s'affranchir de l'autorité judiciaire jugée trop lente ou inapte à faire face à la massification du contentieux. Le rôle du juge est menacé par des propositions de renforcement du rôle des intermédiaires privés (**1**) mais aussi des pouvoirs des autorités administratives dans la lutte contre les contenus illégaux (**2**).

---

(1) François Ewald, « Internet, la fin du journalisme ? », Les Échos, *janvier 2007.*

La Commission juge très dangereuse la tendance du législateur à remédier à des dysfonctionnements de la justice en portant atteinte à des principes de droit. Elle souhaite réaffirmer que **l'intervention d'une autorité judiciaire est nécessaire à chaque fois qu'est en cause une liberté individuelle** et estime, comme le Conseil national du numérique, que « *la préservation de la sécurité publique ne se bâtira pas sur des régimes d'exception et que seule une justice formée et outillée pour faire face à ces nouveaux enjeux liés au numérique sera à même de garantir l'équilibre entre sécurité et libertés publiques et individuelles* » [(1)] (**3**).

1. Limiter le rôle de « censeurs » des intermédiaires privés

La LCEN a défini deux grandes catégories d'acteurs :

– les éditeurs de services sur internet, pleinement responsables des contenus qu'ils mettent en ligne, sont soumis à un régime de responsabilité calqué sur celui de la presse ;

– les hébergeurs bénéficient d'un régime de responsabilité civile et pénale limitée à l'égard des contenus illégaux. Ce régime de responsabilité se fonde sur leur rôle purement passif à l'égard des contenus de tiers qu'ils rendent accessibles sans en prendre connaissance.

La Commission rappelle que ce régime de responsabilité se justifie par le fait qu'il n'est pas souhaitable que la loi délègue aux hébergeurs la censure des communications sur internet en contournant l'autorité judiciaire qui a seule la légitimité de restreindre la liberté d'expression des citoyens en vertu du principe répressif institué avec la loi sur la liberté de la presse en 1881. L'extension de mécanismes de censure privée via la loi contreviendrait au droit à un procès équitable et méconnaîtrait les principes qui sous-tendent l'État de droit.

Face aux propositions et évolutions tendant à renforcer la responsabilité des hébergeurs à l'égard des contenus illégaux, la Commission estime que **le statut de l'hébergeur**, qui constitue une grande conquête et une garantie importante des libertés (libertés d'expression et liberté d'innovation), **doit être réaffirmé** (***a***). Elle considère que le critère du « manifestement illicite » constitue un rempart insuffisant contre le risque de censure privée et mérite d'être clarifié (***b***). Elle est attachée à la réaffirmation des obligations limitées des hébergeurs à l'égard des contenus illégaux (***c***).

---

(1) Conseil national du numérique, Ambition numérique. Pour une politique française et européenne de la transition numérique, *juin 2015, p. 37.*

Dans la même logique, la Commission souhaite que le rôle de *Google*, intermédiaire privé, dans la mise en œuvre du droit au déréférencement consacré par l'arrêt *Google Spain* du 13 mai 2014 par la Cour de justice de l'Union européenne (CJUE) soit précisément encadré, s'agissant de concilier la protection de la vie privée et la liberté d'expression. Ce point sera abordé plus précisément dans la partie III du présent rapport [(1)].

Le rôle des intermédiaires techniques dans la lutte contre les contenus illégaux : état des lieux

La loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004, qui a transposé la directive communautaire 2000/31/CE du 8 juin 2000 sur le commerce électronique, a prévu un régime de responsabilité atténuée applicable aux intermédiaires techniques à l'égard des contenus illicites qu'ils stockent ou acheminent, par opposition aux éditeurs de sites dont le régime de responsabilité est analogue à celui des éditeurs de presse.

L'absence d'obligation générale de surveillance

S'agissant des hébergeurs et des FAI, l'article 6-I-7 consacre l'absence d'obligation générale de surveiller les informations qu'ils transmettent ou stockent et de rechercher des faits ou des circonstances révélant des activités illicites.

Dans deux arrêts du 12 juillet 2012, la Cour de cassation a jugé qu'il ne pouvait être enjoint aux hébergeurs de bloquer la réapparition d'un contenu retiré une première fois en raison de son caractère illicite, car cela équivaudrait à leur imposer une obligation de surveillance générale.

L'obligation de mise en place d'un dispositif de signalement des contenus odieux et des jeux d'argent illégaux

Cependant, compte tenu de l'intérêt général attaché à la répression de certains contenus particulièrement odieux, l'article 6-I-7 de la loi LCEN oblige les FAI et hébergeurs à mettre en place un dispositif facilement accessible et visible permettant à toute personne de leur signaler ce type de contenu, à informer promptement les autorités publiques compétentes en cas de signalement et à rendre publics les moyens qu'ils consacrent à la lutte contre ces activités illicites.

Cette obligation concerne l'apologie des crimes contre l'humanité, l'incitation à la haine raciale, la pornographie enfantine, l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, les atteintes à la dignité humaine. Elle a été étendue aux jeux d'argent illégaux.

L'irresponsabilité sous condition des hébergeurs à l'égard des contenus illégaux

En ce qui concerne les hébergeurs, en application des articles 6-I-2 et 6-I-3 de la LCEN, leur responsabilité civile ou pénale ne peut pas être engagée « *s'ils n'avaient pas effectivement connaissance* » du caractère illicite des contenus stockés ou « *si dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible* ».

Afin de ne pas ériger le fournisseur d'hébergement en juge de l'illicite (et du licite) et de protéger la liberté d'expression et de communication, le Conseil constitutionnel a apporté à cette disposition une réserve d'interprétation, dans une décision du 10 juin 2004, en précisant que les articles 6-I-2 et 6-I-3 de la LCEN « *ne*

(1) Voir infra, *le* a *du 3 du B du III.*

sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers ***si celle-ci ne présente pas manifestement un tel caractère*** *ou si son retrait n'a pas été ordonné par un juge* » [(1)]. Le Conseil constitutionnel précise aux commentaires de cette décision que les hébergeurs ne doivent pas être responsables de tous les contenus dont ils ont connaissance car « *la caractérisation d'un message illicite peut se révéler délicate, même pour un juriste* ». Les hébergeurs, n'ayant ni les compétences ni les moyens pour les caractériser, risqueraient de censurer tout contenu signalé afin de se prémunir de toute mise en cause de leur responsabilité.

L**'hébergeur ne sera donc pas sanctionné pour ne pas avoir retiré un contenu dont le caractère illicite n'est pas manifeste**. Notamment il ne peut être exigé de l'hébergeur, en cas de prétendue contrefaçon, de vérifier la titularité des droits sur l'œuvre. Dans une ordonnance du 4 avril 2013, le juge des référés du tribunal de grande instance rappelle que l'hébergeur n'a pas à apprécier le caractère diffamatoire d'un contenu et que la « *diffamation, à la supposer constituée, n'égale pas forcément trouble manifestement illicite* ».

À l'inverse, le tiers qui dénonce des contenus de manière intempestive peut voir sa responsabilité engagée. En application de l'article 6-I-4, le fait, pour toute personne, de présenter aux hébergeurs un contenu comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion alors qu'elle sait cette information inexacte, est punie d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.

L'article 6-I-5 pose une **présomption de connaissance des faits litigieux lorsque la notification du contenu illicite à l'hébergeur comporte un certain nombre d'éléments** notamment la description des faits litigieux et l'adresse *web* du contenu incriminé, les motifs pour lesquels le contenu doit être retiré et la copie de la première demande de retrait adressée à l'éditeur ou la justification de l'impossibilité de contacter l'éditeur. Les juges ont considéré à plusieurs reprises que si la notification n'avait pas été faite dans les formes, la responsabilité de l'hébergeur ne pouvait pas être engagée avant de considérer que la loi n'impose pas de recourir à la procédure de notification pour informer les hébergeurs.

Le rapport de Marc Robert sur la cybercriminalité indique que ce dispositif a été investi par l'autorité publique. « *De telles demandes, qui relèvent alors de la police administrative, peuvent viser aussi bien des hébergeurs étrangers que français ; elles sont généralement satisfaites à l'heure actuelle lorsque l'infraction visée concerne le racisme, la pédopornographie ou l'escroquerie. Il s'agit toutefois d'une simple obligation de moyens, dans la mesure où l'hébergeur peut s'exonérer de toute responsabilité s'il justifie que l'auteur ou l'éditeur de la page concernée a été invité à retirer ou à modifier le contenu faisant grief* » [(2)].

(1) Décision n° 2004-496 DC du 10 juin 2004, Loi pour la confiance dans l'économie numérique, *considérant 9.*

(2) Groupe de travail interministériel sur la lutte contre la cybercriminalité, Protéger les internautes. Rapport sur la cybercriminalité, *février 2014, p. 185.*

a. Les incertitudes sur la ligne de démarcation entre hébergeur et éditeur et l'objectif de « régulation des plateformes » n'appellent pas la création d'une nouvelle catégorie dans la LCEN

Le Conseil d'État, dans son étude annuelle 2014, estime que « *la* summa divisio *issue de la directive sur le commerce électronique est aujourd'hui sujette à de fortes incertitudes quant à la démarcation entre les deux catégories d'éditeur et d'intermédiaire technique* » et qu'« *il est probable que dans les prochaines années, des décisions juridictionnelles écarteront la qualification d'hébergeur pour les principales catégories de plateformes (…) : après les places de marché et les moteurs de recherche, suivront les réseaux sociaux, les plateformes de partage et les magasins d'applications. Tous ces acteurs perdront alors le régime de responsabilité limitée qui favorise leur activité* » (1).

Le Conseil d'État propose par conséquent de **définir une catégorie des plateformes**, distincte de celle des hébergeurs, mais qui, **à l'égard des contenus mis en ligne par les tiers,** se verrait appliquer **le régime de responsabilité civile et pénale des hébergeurs.** Seraient qualifiés de plateformes les services de référencement ou de classement de contenus, biens ou services édités ou fournis par des tiers et partagés sur le site de la plateforme (moteurs de recherche, réseaux sociaux, sites de partage de contenus, places de marché, magasins d'applications, agrégateurs de contenus et comparateurs de prix). Par rapport aux hébergeurs, les plateformes se distingueraient donc par l'existence d'un **service de classement ou de référencement**.

La création d'une nouvelle catégorie des plateformes entre hébergeurs et éditeurs poursuit un double objectif pour le Conseil d'État :

– **un objectif de préservation de la liberté d'expression**. Pour le Conseil, la remise en cause par la jurisprudence de la qualification d'hébergeur pour certaines plateformes serait dangereuse parce que le régime de responsabilité limitée est protecteur de la liberté d'expression. C'est pourquoi l'étude annuelle 2014 propose de les faire entrer dans une nouvelle catégorie qui leur garantirait de plein droit le régime de responsabilité limitée ;

– **un objectif de régulation accrue de l'activité des plateformes**. Parallèlement, le Conseil souhaite imposer de nouvelles obligations à ces intermédiaires, non pas à l'égard des contenus illégaux, mais à l'égard de leurs utilisateurs finaux et des tiers qui mettent en ligne leurs contenus, en matière de pertinence de leur classement.

La Commission partage les objectifs généraux poursuivis mais ne partage pas l'approche du Conseil d'État.

---

(1) Conseil d'État, op. cit., *p. 221.*

En ce qui concerne **l'objectif de régulation des plateformes, la Commission estime qu'il ne passe pas par la création d'une nouvelle catégorie au sein de la LCEN**.

La Commission rappelle que les catégories d'hébergeurs et d'éditeurs ont pour finalité exclusive de définir les régimes de responsabilité qui doivent s'appliquer aux acteurs de l'internet **à l'égard des contenus illégaux**. Il ne s'agit donc **pas du bon vecteur** pour définir une nouvelle catégorie dont on souhaite renforcer certaines obligations à l'égard des utilisateurs finaux et des tiers dans la pertinence de leurs outils de classement. La Commission identifie un risque de confusion des finalités.

De fait, la classification proposée par le Conseil d'État n'apparaît pas pertinente.

D'une part, il serait peu lisible de créer une nouvelle catégorie pour lui appliquer le même régime de responsabilité que celui des hébergeurs.

D'autre part, si l'on peut défendre que les « plateformes » se distinguent des hébergeurs « passifs » par l'utilisation d'outils de classement et de référencement pour leur imposer des obligations à cet égard, il convient de rappeler que **de nombreux éditeurs utilisent aussi de tels outils de classement et de référencement. Il ne semble donc ni pertinent ni justifié d'imposer aux plateformes des obligations de loyauté à l'égard des utilisateurs finaux qui ne s'appliqueraient pas aux éditeurs utilisant les mêmes outils**. La catégorie juridique des plateformes telle que définie par le Conseil d'État présente le défaut de ne pas permettre d'appréhender des plateformes telles que *Netflix*, *Deezer*, *Spotify*, *iTunes*, *Amazon*, qui ont une responsabilité dans la production ou la sélection de contenus et qui échapperaient *de facto* à l'obligation de « loyauté ».

La Commission reviendra plus en détail sur les enjeux de la régulation des plateformes dans la partie IV du présent rapport [(1)].

En ce qui concerne l'objectif de défense de la liberté d'expression, la Commission estime que **le risque**, identifié par le Conseil d'État, **qu'à moyen terme, tous les grands services d'intermédiation utilisés sur internet perdent la qualification d'hébergeur et le régime de responsabilité limitée qui en découle n'est pas avéré** (voir l'encadré ci-après). En ce qui concerne les incertitudes soulignées par le Conseil d'État dans la qualification des acteurs, elles sont incontournables dans un contexte d'évolution particulièrement rapide des services rendus par les intermédiaires de l'économie numérique. Elles ne seraient que renforcées par la création d'une troisième catégorie d'acteur dont les frontières avec l'hébergeur et l'éditeur seraient encore plus difficiles à définir.

---

(1) Voir infra, *le C du IV.*

Un statut d'hébergeur largement reconnu aux plateformes du *web 2.0* par la jurisprudence

Il est vrai que depuis l'adoption de la LCEN, le développement de l'internet interactif dit *web 2.0* a entraîné l'apparition de nouveaux acteurs dont la passivité et la neutralité ont pu être sujettes à discussion et pour lesquels s'est posée la question de leur responsabilité à l'égard du contenu qu'ils hébergent. Il s'agit des sites dits *« collaboratifs »* reposant sur le partage de contenus (type *Dailymotion, Youtube* ou *Facebook*), ainsi que des plateformes de vente aux enchères (type *eBay* ou *Priceminister*). Ces sites ont été à l'origine de nombreuses décisions commentées pour leurs contradictions, les différents sites étant alternativement qualifiés d'éditeur ou d'hébergeur.

La jurisprudence a pourtant retenu la qualification d'hébergeur pour les sites collaboratifs ou participatifs tels *Wikipedia, Myspace* ou *Facebook*.

Les solutions ont été plus fluctuantes s'agissant des sites de partage de vidéos. Si dans un premier temps, les juges ont pu opter pour la qualification d'éditeur [(1)], **l'ensemble des sites de partage de vidéos est désormais qualifié d'hébergeur**. Dans deux arrêts *Google* du 23 mars 2010, la CJUE a précisé que l'hébergeur doit avoir un rôle neutre, « *purement technique, automatique et passif.* » Par application de ces critères, la Cour de cassation a reconnu le statut d'hébergeur à *DailyMotion* en 2011 [(2)]. **La même qualification a été retenue pour les sites agrégateurs d'information**.

La qualification des places de marché en ligne telles que le site *eBay* fait débat. Dans un arrêt *L'Oréal c. eBay*, la Cour de justice de l'Union européenne a jugé que le statut d'hébergeur ne pouvait s'appliquer à un site de place de marché que si celui-ci ne joue pas « *un rôle actif qui lui permette d'avoir une connaissance ou un contrôle des données stockées* » et que « *ledit exploitant joue un tel rôle quand il prête une assistance laquelle consiste notamment à optimiser la présentation des offres à la vente en cause et à promouvoir celles-ci* » (CJUE, *L'Oréal SA et autres contre eBay International AG et autres*, 12 juillet 2011, n° C-324/09). Dans une autre affaire concernant *eBay*, la Cour de cassation a repris le même raisonnement et confirmé l'arrêt de la cour d'appel de Paris écartant la qualification d'hébergeur (Cass. com., 3 mai 2012, n° 11-10.508).

Les sociétés *Louis Vuitton Malletier* et *Christian Dior Couture* reprochaient notamment à *eBay* de favoriser des actes de contrefaçon de leurs marques et ainsi de commettre des actes illicites.

En substance, la Cour de cassation relève qu'*eBay* :

– fournit à l'ensemble des vendeurs des informations leur permettant d'optimiser leurs ventes ;

– assiste les vendeurs dans la description des objets mis en vente ;

– propose aux vendeurs de créer un espace personnalisé de mise en vente voire même de bénéficier « d'assistants vendeurs » ;

– envoie des messages invitant l'enchérisseur qui n'a pu remporter une enchère à se reporter sur d'autres objets similaires.

Dans ces conditions, la Cour de cassation considère qu'*eBay* a joué un *rôle actif* indépendamment de toute option choisie par les vendeurs, en sorte que la plateforme de commerce électronique ne peut prétendre au statut d'hébergeur.

Le statut des moteurs de recherche, dont la responsabilité à l'égard des contenus illégaux auxquels ils renvoient n'a pas été prévue par la LCEN, fait également l'objet de débats. La jurisprudence se montre particulièrement fluctuante sur le statut de *Google* pour

son service *Adwords*. Saisie sur renvoi préjudiciel de la Cour de cassation de la qualification du service de référencement *Adwords* de *Google*, la CJUE a appliqué le même critère du « rôle actif » ; tout en laissant au juge national le soin de qualifier le service de *Google*, la CJUE a relevé que « Google *procède, à l'aide des logiciels qu'elle a développés, à un traitement des données introduites par des annonceurs et qu'il en résulte un affichage des annonces sous des conditions dont* Google *a la maîtrise* » et que « Google *détermine l'ordre d'affichage, en fonction, notamment, de la rémunération payée par les annonceurs* » (CJUE, 23 mars 2010, *Google France et Google Inc c. Louis Vuitton Malletier*, n° C-236/08, § 115). Néanmoins **dans un arrêt du 9 avril 2014, la Cour d'appel de Paris a confirmé le statut d'hébergeur de *Google* pour son service *Google Adwords***.

S'agissant du service de recherche « naturelle », le TGI de Paris, dans un jugement du 6 novembre 2013, a écarté la qualification d'hébergeur et retenu, en se fondant sur des documents émanant d'ailleurs de la société *Google* elle-même, l'existence d'un « choix éditorial » quant aux classements des contenus, la société ayant une entière liberté dans la détermination de son algorithme [(3)].

(1) CA Paris, 7 juin 2006, Tiscali Média c. Dargaud Lombard et Lucky Comics *; Cass. 1ère civ., 14 janvier 2010, n° 06-18.855.*

(2) Cass. 1re civ., 17 février 2011, n° 09-67896.

(3) TGI Paris, Mosley c. Google Inc., *n° 11/07970.*

En outre, la Commission s'interroge sur la légitimité de garantir de plein droit à l'ensemble des « plateformes » un régime de responsabilité limitée au nom de la liberté d'expression. Une approche jurisprudentielle permettant d'apprécier la qualité de l'intermédiaire (hébergeur ou éditeur) au cas par cas lui semble préférable.

En effet, dans les cas limités où la jurisprudence a refusé le statut d'hébergeur à l'activité d'une plateforme, en l'occurrence *eBay*, le rôle actif de la plateforme a été largement établi à l'égard du contenu fourni lui-même (voir l'encadré ci-dessus).

En outre, en ce qui concerne *eBay* et les places de marché en général, on ne saurait défendre l'application de plein droit d'un régime de responsabilité limitée au nom de la liberté d'expression. Il en va de même des comparateurs de prix ou des magasins d'applications auxquels le Conseil d'État propose d'attribuer de plein droit un régime de responsabilité limitée, à travers l'attribution du statut de plateforme.

La question de *Google*, dont la responsabilité en tant que responsable de traitement de données personnelles a été renforcée par l'arrêt *Google Spain* du 13 mai 2014 de la CJUE, doit sans doute faire l'objet d'une approche particulière, à travers notamment l'encadrement du droit à l'oubli et le droit de la concurrence.

En tout état de cause, si le statut de l'hébergeur devait être remis en cause par la jurisprudence d'une manière qui menacerait la liberté d'expression, il serait préférable de repréciser la définition de l'hébergeur plutôt que de créer une nouvelle catégorie intermédiaire, qui, en souhaitant clarifier les lignes de partage,

risque de créer encore plus d'incertitude et de complexité dans la qualification des acteurs.

Recommandation n° 22

Réaffirmer la dichotomie entre éditeur et hébergeur et réaffirmer la responsabilité limitée de l'hébergeur, garante de la liberté d'expression et de la liberté d'innovation.

Ne pas créer de catégorie intermédiaire des « plateformes » entre l'hébergeur et l'éditeur.

b. Le critère du « manifestement illicite » : un rempart insuffisant contre la censure privée

En revanche, en matière de liberté d'expression, la Commission estime que l'une des faiblesses du régime actuel réside dans la difficulté à déterminer ce qui est « manifestement illicite ». Cette difficulté pourrait inciter les hébergeurs à censurer des contenus au-delà de ce que leur impose la loi. Comme l'a indiqué Mme Marie Mongin, vice-présidente de la 17e chambre du TGI de Paris, lors de son audition du 3 juillet 2014, « *en ce qui concerne le régime de responsabilité de l'hébergeur, l'équilibre n'est sans doute pas si mauvais que cela, même s'il n'est pas facile d'apprécier ce qui est manifestement illicite, en particulier pour des contenus qui relèvent de l'opinion* ».

Pour la Quadrature du net, « *l'interprétation extensive du critère de «* manifestement illicite *» par les juges du fond depuis 2004 a conduit à la situation que le Conseil (constitutionnel) avait tenté d'éviter : la majorité des hébergeurs, incapables d'évaluer le caractère manifestement illicite des contenus qui leur sont signalés, sont incités à supprimer la plupart de ces contenus, en dehors de tout cadre judiciaire, afin de s'exonérer de tout risque juridique (voir l'affaire jugée le 11 juin 2013 par le TGI de Brest, où la société d'hébergement* Overblog *est condamnée à 10 000 euros d'amende pour ne pas avoir retiré un contenu dont le tribunal estime qu'il était «* manifestement illicite *» tout en n'étant pas «* certainement illicite » » [(1)].

M. Benoît Tabaka, directeur des politiques publiques de *Google France*, estime également qu'au gré des contentieux, « *il semble que l'appréciation du caractère manifestement illicite d'un contenu ait disparu et clairement, il est de moins en moins dans l'intérêt d'un intermédiaire de remettre en cause ce caractère manifeste dans ses échanges avec les tiers* ». Se pose donc selon lui la question suivante : « *le garde-fou créé par le Conseil constitutionnel destiné à éviter les notifications abusives et destiné, non pas à protéger les intermédiaires*

---

(1) La Quadrature du net, Projet de loi sur l'égalité entre les hommes et les femmes : non à la censure privée du net, *15 janvier 2014.*

mais à assurer la protection de la liberté de communication, est-il toujours effectif ? » [1]

Cette affirmation rejoint les observations de M. Edwy Plenel lors de la table ronde du 3 juillet : « [n]*ous sommes concrètement saisis sur des billets de blogs d'opinion par les personnes qui sont visées par ces opinions et qui en demandent la dépublication. Dans l'état actuel de la jurisprudence, nous devons, après avoir prévenu l'auteur, dépublier la contribution, à défaut de quoi nous devenons solidaires du contenu et sommes poursuivis en tant que responsables de sa diffusion. Nous le faisons à condition naturellement que la demande de dépublication soit formulée dans les formes, qu'elle ne soit pas automatique ou qu'elle ne requiert pas la censure pure et simple. Mais nous sommes* de facto *amenés à faire nous-mêmes la censure d'une opinion qui ne devrait se jouer que devant le juge* (…) *Il y a là une zone grise de la liberté d'expression* ». M. Edwy Plenel s'est exprimé sur la nécessité de « *réaffirmer le statut de l'hébergeur* ». Il a estimé que le droit actuel n'était pas suffisamment protecteur de la liberté d'expression en ce qu'il mettait l'hébergeur qu'est *Mediapart* en situation de censurer des opinions en dehors de toute intervention d'un juge.

Lors de la même table ronde, M. Giuseppe di Martino, secrétaire général de *Dailymotion* et président de l'Association des services Internet communautaires (ASIC), a également indiqué que *DailyMotion* était amené à retirer des propos relevant de l'opinion et non manifestement illicites : « [e]*n dehors des contenus manifestement illicites, nous avons tendance à refuser les demandes de retrait. Mais si les choses s'enveniment et que nous sentons que le débat va être sans fin, de guerre lasse, nous retirons le contenu. Il n'y a donc pas d'automaticité.* » Face à une demande de retrait d'un contenu au motif qu'il serait diffamatoire, « *en tant que bons parents, on le fait ou pas… Il n'y pas d'automaticité à la différence de ce que peut faire* Mediapart. *Tels propos sur la politique expansionniste d'Israël vont être jugés inacceptables par certains mais pas par d'autres. Nous sommes entre le marteau et l'enclume. Si nous voyons que les choses s'enveniment, nous les retirons.* »

La Commission estime par conséquent qu'il serait nécessaire que le législateur reprécise cette notion de « *manifestement illicite* », qui comporte une dimension morale, en lui substituant la notion de « *manifestement illégal* ».

La Commission serait également favorable à **l'introduction du principe du contradictoire dans le retrait de contenus illégaux**. Le Conseil national du numérique propose à cet égard de faire intervenir la plateforme PHAROS afin que l'hébergeur ne soit plus l'unique juge du « *manifestement illicite* ». Lorsqu'un contenu contraire à la loi est signalé par un individu, son signalement serait transmis sans délai à l'hébergeur ainsi qu'à PHAROS. Dans le même temps, l'auteur du contenu litigieux serait informé du signalement et du fait qu'il peut présenter ses observations dans un délai raisonnable. Ces observations seraient

---

(1) Benoît Tabaka, « Une histoire d'hébergeurs », Owni, *août 2011.*

transmises à PHAROS ainsi qu'à la plateforme. Dès réception du signalement, la plateforme examinerait le contenu. Si celui-ci est manifestement illicite, elle le retirerait temporairement en attendant la confirmation formelle de PHAROS en charge du traitement approfondi du signalement. Le cas échéant, après avoir pris connaissance des éventuelles observations de l'auteur du contenu, PHAROS confirmerait ou non le caractère manifestement illicite du contenu et se réserverait l'opportunité de transmettre le dossier au parquet. À défaut de confirmation, le contenu serait réintégré sur la plateforme.

S'agissant des suppressions de contenus par des hébergeurs à la demande de tiers, la Commission souhaite qu'il puisse y avoir **une transparence sur les mesures prises à travers la mise en place d'une base de données des notifications**. Le Conseil national du numérique propose à cet égard la création d'une plateforme recensant les retraits de contenus en format libre et ouvert. Cette plateforme permettrait aux citoyens de disposer d'informations fiables et transparentes sur l'étendue et la nature des retraits effectués à la suite de signalements par des tiers ou par l'autorité administrative.

Recommandations n°s 23 à 25

– n° 23 : substituer dans la législation la notion plus objective de « manifestement illégal » à celle de « manifestement illicite » ;

– n° 24 : introduire le principe du contradictoire dans le retrait de contenus illégaux. Faire intervenir la plateforme PHAROS afin que l'hébergeur ne soit plus seul juge du « manifestement illicite » ;

– n° 25 : assurer la transparence des suppressions de contenus par les hébergeurs à travers la mise en place d'une base de données des notifications et retraits en format libre et ouvert.

c. Réaffirmer les obligations limitées des hébergeurs dans la lutte contre les contenus illégaux

De nombreuses voix s'élèvent aujourd'hui pour exiger un renforcement de la responsabilité des intermédiaires de l'internet dans la lutte contre les contenus illégaux fournis par des tiers (voir l'encadré ci-après).

Il est notamment proposé :

– d'imposer de nouvelles obligations de surveillance à l'ensemble des hébergeurs ;

– ou de créer une nouvelle catégorie intermédiaire entre l'hébergeur et l'éditeur dans l'objectif de lui imposer des obligations de surveillance accrues à l'égard des contenus illégaux.

De nombreux acteurs appellent de leurs vœux un renforcement des obligations des intermédiaires privés dans la lutte contre les contenus illégaux

Cette position est défendue par les ayants droit, certaines associations de lutte contre les discriminations mais aussi de nombreuses personnalités politiques ou institutions publiques.

Le **Conseil d'État** dans son étude annuelle propose par exemple d'imposer aux hébergeurs (comme aux plateformes) une **obligation d'empêcher, durant un délai déterminé, la réapparition des contenus ayant précédemment fait l'objet d'un retrait**. Cette obligation serait **prononcée par l'autorité administrative**. Cette proposition avait été formulée antérieurement par un rapport de Mme Mireille Imbert-Quaretta sur la lutte contre la contrefaçon en ligne remis en mai 2014 à la ministre de la culture. Comme l'indique ce rapport, « *la réapparition des contenus supprimés constitue la principale limite des procédures de notification des contenus contrefaisants hébergés sur les sites. Les ayants droit, qui ont recours à la notification prévue à l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, sont confrontés à la réapparition permanente des contenus et des liens dont ils demandent le retrait* » (1).

Le **rapport de M. Marc Robert sur la cybercriminalité** souhaite également obliger les moteurs de recherche, les hébergeurs et les FAI à **détecter préventivement les infractions les plus graves**. Il vise spécialement celles de l'article 6-I-7 de la LCEN, à savoir l'apologie des crimes contre l'humanité, l'incitation à la haine raciale, la pornographie enfantine, l'incitation à la violence et les atteintes à la dignité humaine. Cette obligation de surveillance préventive ne viserait que les infractions « *se prêtant techniquement à une telle détection* ».

Un **rapport d'information** de février 2011 des sénateurs Laurent Béteille et Richard Yung consacré à la **lutte contre la contrefaçon** proposait de créer un statut intermédiaire entre ceux d'éditeur et d'hébergeur, qui s'appliquerait potentiellement à la majorité des services *web* et leur imposerait **une obligation de surveillance des contenus**.

S'il n'a pas repris cette idée dans son rapport final, M. Pierre Lescure avait annoncé lors du bilan de mi-parcours de la mission Acte 2 qu'il allait « *falloir revenir sur la définition d'un certain nombre de statuts d'aujourd'hui, à commencer par celui d'hébergeur* ». « *Un hébergeur aujourd'hui ne peut plus revendiquer la même neutralité qu'au début de son activité* ». Il avait annoncé souhaiter réfléchir à la définition d'un statut intermédiaire entre l'hébergeur et l'éditeur.

En janvier dernier, dans une interview aux *Échos* , **la ministre de la culture, Mme Fleur Pellerin** s'est exprimée pour la création d'un statut hybride entre l'éditeur et l'hébergeur, plus contraignant que celui de l'hébergeur, pour appréhender les plateformes qui éditorialisent en partie les contenus proposés comme *Youtube*, *Dailymotion* ou *Facebook* (2).

L'avis de la **CNCDH** sur la lutte contre les discours de haine sur internet propose également d'imposer aux prestataires qui jouent un rôle actif sur les contenus mis en ligne par le biais de services de référencement ou de classement une « *obligation de détection préventive (proactive) des contenus susceptibles de constituer une infraction relative aux abus de la liberté d'expression, (…) notamment par le biais d'algorithmes basés sur les vecteurs sémantiques et les contextes* » (3).

(1) Mireille Imbert-Quaretta, Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne, *mai 2014, p. 16.*

(2) http://www.lesechos.fr/tech-medias/hightech/0204176550591-le-statut-dhebergeur-au-coeur-des-debats-1095608.php

(3) CNCDH, Avis sur la lutte contre les discours de haine sur internet, *12 février 2015, § 18.*

À l'appui de ces propositions, **sont mises en avant les limites d'un recours systématique au juge** compte tenu notamment de l'ampleur des infractions sur internet et de son incapacité à répondre au problème de la prolifération des sites miroirs.

L'absence d'obligation de surveillance des hébergeurs est également contestée au regard des évolutions technologiques et notamment du **développement, postérieur à la LCEN, de technologies de reconnaissance des contenus** (*data mining, fingerprinting, tags*…) qui permettraient d'accroître les obligations de surveillance des intermédiaires.

Enfin, ces propositions s'appuient sur l'idée que certains acteurs qualifiés d'hébergeurs, notamment les plateformes de partage de vidéos, auraient en réalité **un rôle « actif »** sur les contenus mis en ligne, notamment par le biais de services de référencement ou de classement, voire de recommandation, qui justifierait des obligations supplémentaires à l'égard de ces contenus.

La Commission, attachée au rôle du juge, n'est pas favorable au renforcement par la loi des obligations de surveillance des intermédiaires privés dans la lutte contre les contenus illégaux, ni à la création d'un statut intermédiaire entre l'éditeur et l'hébergeur, soumis à un régime de responsabilité renforcée.

S'agissant du rôle actif que joueraient certains hébergeurs par leurs systèmes de référencement ou de classement, la Commission rappelle que la responsabilité limitée de ces acteurs résulte en réalité de ce qu'**ils n'ont pas connaissance des contenus**, contrairement aux éditeurs. Le fait que certains hébergeurs aient recours à des outils de classement des contenus mis en ligne par des tiers peut justifier d'imposer des règles en ce qui concerne ce classement mais ne justifie pas que la loi leur impose des obligations de surveillance et de censure supplémentaires sur ces contenus.

En ce qui concerne les outils de reconnaissance des contenus, comme l'a rappelé, M. Giuseppe Di Martino, secrétaire général de *Dailymotion* et président de l'Association des services Internet communautaire (ASIC), lors de son audition du 3 juillet 2014, si **le *finger printing*** peut être un moyen efficace de retirer des contenus dont les ayants droit n'acceptent pas la présence chez les hébergeurs, cette technologie **ne permet pas de reconnaître des opinions, des propos, des contenus diffamatoires ou d'incitation à la violence ou à la haine et de les filtrer *a priori***. Le développement de cette technologie ne saurait donc justifier la remise en cause du statut de l'hébergeur et les objectifs de préservation de la liberté d'expression et la liberté d'innovation dont il est le garant.

S'agissant de l'obligation de retrait prolongé d'un contenu reconnu comme illégal, la Commission rappelle que les juridictions françaises peuvent prononcer de telles injonctions, en particulier en référé dans le cadre de l'article L. 336-2 du code de la propriété intellectuelle. Ces injonctions ne sont possibles qu'à condition

de ne pas constituer une obligation générale de surveillance, prohibée par l'article 15 de la directive 2000/31 sur le commerce électronique. L'obligation mise à la charge de l'hébergeur ou de la plateforme doit donc être strictement proportionnée, limitée dans le temps, ciblée sur des contenus précis, et mise en œuvre de façon à ne pas constituer une « surveillance généralisée ». La Commission estime que **de telles injonctions ont vocation à être prononcées par un juge et n'est pas favorable à la proposition formulée par les rapports du Conseil d'État et de Mme Mireille Imbert-Quaretta de permettre à l'autorité administrative de les prononcer**.

De manière générale, la Commission souhaite mettre en garde contre les tentations de contournement de l'autorité judiciaire par des autorités administratives dans la lutte contre les contenus illégaux.

Recommandation n°s 26 et 27

– n° 26 : ne pas renforcer par la loi les obligations de surveillance des intermédiaires techniques ;

– n° 27 : réserver au juge la faculté de prononcer des injonctions de retrait prolongé de contenus illégaux.

2. Limiter les cas de contournement du juge par les autorités administratives

De manière générale, face aux lenteurs et aux inadaptations de la justice, l'objectif de lutte contre la prolifération de contenus illégaux dans l'univers numérique débouche sur **des propositions controversées de renforcement des pouvoirs des autorités administratives pour prononcer des mesures restrictives de la liberté d'expression**. Ces propositions font débat en ce qu'elles confèrent à une autorité administrative, fût-elle indépendante, un pouvoir extra-judiciaire de régulation de contenus.

Cette question a déjà été abordée par la Commission lorsqu'elle a exprimé une position sur le blocage sur décision administrative des contenus incitant au terrorisme autorisé par l'article 12 de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. Dans sa recommandation du 22 juillet 2014, la Commission **a rappelé que l'intervention d'une autorité judiciaire est nécessaire à chaque fois qu'est en cause une liberté individuelle** afin de s'assurer que la mesure prise ne présente pas de caractère arbitraire, qu'elle est nécessaire et proportionnée à l'objectif poursuivi et respecte les droits de la personne [(1)] (***a***). Plus généralement, elle appelle à une limitation des cas de contournement du juge par les autorités administratives (***b***).

---

(1) Voir la recommandation du 22 juillet 2014 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme.

a. N'autoriser le blocage qu'à titre subsidiaire et sur décision judiciaire

La Commission estime que la multiplicité et la confusion des initiatives législatives en matière de blocage imposent l'élaboration d'une doctrine claire sur ce sujet (voir l'encadré ci-après). Dans sa recommandation du 22 juillet 2014, la Commission s'est exprimée clairement et à l'unanimité pour que le blocage ne soit autorisé qu'à titre subsidiaire et sur décision judiciaire.

La multiplicité et la confusion des initiatives législatives en matière de blocage imposent l'élaboration d'une doctrine claire sur ce sujet

Au cours des dernières années, les initiatives législatives visant à permettre le blocage de sites se sont multipliées.

En ce qui concerne le **blocage judiciaire**, l'**article 6-I-8 de la LCEN** dispose que l'autorité judiciaire peut prescrire en référé ou sur requête aux hébergeurs ou, à défaut, aux FAI toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.

L'**article L. 336-2 du code de la propriété intellectuelle**, introduit par la loi Hadopi, dispose qu'« *en présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de grande instance, statuant le cas échéant en la forme des référés, peut ordonner (…) toutes mesures propres à prévenir ou à faire cesser une telle atteinte (…)* ».

Un **blocage « hybride »** (judiciaire à l'initiative d'une autorité administrative indépendante) des sites de jeux illégaux a été mis en place par la **loi du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne**.

Il n'existe aujourd'hui que deux dispositifs de **blocage administratif** (article 6-I-7 de la LCEN) :

– le premier, introduit par la **loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure** (LOPPSI 2), concerne les **sites à caractère pédopornographique**. Dans sa décision du 10 mars 2011 sur la LOPPSI 2, le Conseil constitutionnel a validé la procédure de blocage administratif des sites pédopornographiques compte tenu de son caractère proportionné, de la nature de son objet et de la possibilité de recours devant un juge. En 2014, il n'avait pourtant jamais été mis en œuvre en l'absence de décret d'application ;

– le second a été introduit par la **loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme** et concerne les **contenus faisant l'apologie du terrorisme ou provoquant directement au terrorisme**.

L'article 12 de cette loi précise les modalités d'application de ces deux dispositifs. L'autorité administrative transmet les demandes de retrait à une personnalité qualifiée, désignée en son sein par la CNIL, personnalité qui ne peut être un parlementaire. « *La personnalité qualifiée s'assure de la régularité des demandes de retrait et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste. Si elle constate une irrégularité, elle peut à tout moment recommander à l'autorité administrative d'y mettre fin. Si l'autorité administrative ne suit pas cette recommandation, la personnalité qualifiée peut saisir la juridiction administrative compétente, en référé ou sur requête* ».

La personnalité qualifiée « *rend public chaque année un rapport d'activité sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de*

demandes de retrait, le nombre de contenus qui ont été retirés, les motifs de retrait et le nombre de recommandations faites à l'autorité administrative. Ce rapport est remis au Gouvernement et au Parlement ». Un décret d'application du 6 février 2015 est venu préciser les modalités de ce dispositif.

L'article 18 de la LCEN qui permettait à l'autorité administrative de restreindre, dans des cas limitativement énumérés, le libre exercice du commerce électronique a été abrogé par la loi du 17 mars 2014 relative à la consommation. De même, les dispositions de la proposition de loi renforçant la lutte contre le système prostitutionnel qui introduisaient un nouveau cas de blocage administratif ont été supprimées par l'Assemblée nationale en première puis en deuxième lectures.

La Commission s'est interrogée « *sur le caractère adéquat, nécessaire et proportionné de la proposition de blocage administratif, sans contrôle préalable de l'autorité judiciaire, dans le domaine très spécifique de la lutte contre le terrorisme* ».

Elle s'est en particulier **inquiétée du fait que la notion « *d'apologie du terrorisme* » puisse être interprétée de façon extensive si sa réalité n'est pas soumise à l'appréciation préalable du juge judiciaire**.

La Commission a estimé « *que les notions de provocation à des actes de terrorisme et d'apologie de ces actes sont particulièrement délicates à qualifier et que cette qualification ne saurait relever que du juge en raison des risques importants d'atteinte à la liberté d'expression et de communication. La frontière entre la provocation au terrorisme et la contestation de l'ordre social établi peut en effet être particulièrement difficile à tracer car, comme l'a rappelé la Cour européenne des droits de l'homme (CEDH) dans l'arrêt* Association Ekin c. France *du 17 juillet 2001, la liberté d'expression protège* "non seulement les informations ou idées accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi celles qui heurtent, choquent ou inquiètent" ».

L'apologie du terrorisme, une notion particulièrement difficile à cerner et dont la qualification ne saurait relever que d'un juge

La salve de condamnations qui a suivi les attentats de janvier 2015 en application des nouvelles dispositions réprimant l'apologie du terrorisme et la provocation au terrorisme a confirmé les craintes de la Commission sur le **caractère particulièrement flou et potentiellement extensif** des notions d'apologie du terrorisme et de provocation directe au terrorisme [(1)] et la difficulté à cerner cette notion. Le fait de louer directement les attentats perpétrés par les frères Kouachi ou Amedy Coulibaly est-il constitutif d'un message d'apologie ? *A priori*, oui. Mais est-ce que dire « *Je suis Charlie Coulibaly* », comme l'a fait Dieudonné sur son *Facebook* au lendemain des attentats, relève à proprement parler de ce délit ? C'est moins certain. **Cette appréciation ne saurait en tout cas relever que d'un juge**.

En outre, se pose la question de la **limite entre la caractérisation de l'apologie de terrorisme et le pur droit à l'information** : poster la vidéo de l'interview *post-mortem* d'Amedy Coulibaly peut dans certains cas être considéré comme une apologie des actes qu'il a perpétrés ; cela peut aussi viser à dénoncer les justifications que le terroriste apporte à ses actes. Dans cette optique, comment justifier le blocage de cette vidéo ? Ce dispositif est à

double tranchant : il ne doit pas aboutir à une désinformation, alors que le but est de sensibiliser chacun à la lutte contre le terrorisme, ce qui doit forcément passer par l'enseignement de ce qu'est le terrorisme et des procédés employés par les terroristes. Pour prétendre contrer une idée, encore faut-il savoir de quoi l'on parle.

(1) http://tempsreel.nouvelobs.com/charlie-hebdo/20150120.OBS0370/apologie-du-terrorisme-une-longue-liste-de-condamnations.html

Pour l'étude d'impact du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, le blocage administratif présente l'avantage de pouvoir traiter un grand nombre de sites ou de pages internet dans des délais plus brefs que ceux résultant du blocage judiciaire. Cette étude souligne également **les limites d'un recours exclusif au blocage judiciaire** prévu aux articles 6-I-8 et 50-I de la LCEN et aux référés de droit commun prévus aux articles 145, 808 et 809 du code de procédure civile. « *Compte tenu du nombre croissant de sites mis en cause, les juges des référés ne seraient pas en mesure d'intervenir utilement dans des délais restreints. En outre il n'appartiendrait qu'aux seules personnes ayant un intérêt à agir, et non à l'autorité judiciaire d'enclencher cette procédure. Enfin, seuls les sites visés dans la procédure judiciaire pourraient être bloqués, et non les sites miroirs, souvent très nombreux, ce qui limiterait considérablement l'efficacité de l'action judiciaire* ».

De manière générale, la Commission a rappelé « *que* ***le préalable d'une décision judiciaire*** *apparaît comme un* ***principe essentiel****, de nature à respecter l'ensemble des intérêts en présence, lorsqu'est envisagé le blocage de l'accès à des contenus illicites sur des réseaux numériques. Ce préalable constitue une garantie forte de la liberté d'expression et de communication et de la neutralité des réseaux* ».

La Commission **a également contesté la nécessité de contourner le juge**, en constatant « *que sur les 360 signalements effectués en 2013 par les internautes et les services de police auprès de la plateforme PHAROS, 122 constituent des cas avérés de provocation au terrorisme ou d'apologie du terrorisme. Compte tenu de ces éléments et sauf autre indication de nature à modifier significativement le nombre de signalements effectifs, le risque d'engorgement des tribunaux mis en avant par le Gouvernement à l'appui du blocage administratif ne lui apparaît pas établi* ».

La Commission s'est par ailleurs interrogée sur **l'adéquation et la pertinence du dispositif proposé pour la réalisation de l'objectif poursuivi** :

– d'une part, la Commission a rappelé qu'en l'état actuel des technologies, un même serveur pouvant héberger plusieurs contenus, les solutions de blocage sont susceptibles d'entraîner du sur-blocage, c'est-à-dire le blocage de contenus légaux autres que ceux visés, ce qui constitue une atteinte à la liberté d'expression et de communication de tiers. « *Ce risque est important dans le cas présent puisque 90 % des contenus de provocation au terrorisme et d'apologie du terrorisme semblent se situer sur des réseaux sociaux ou des plateformes de partage de vidéos comme* Youtube *ou* Dailymotion. *Compte tenu de ce risque, il*

est à craindre que les mesures de blocage ne concernent en pratique que 10 % des contenus en cause ». De fait, le mode de blocage retenu par le décret d'application du 6 février 2015 est un blocage par DNS (nom de domaine), ce qui signifie que le blocage s'applique à des sites entiers. Il est donc en pratique inapplicable aux plateformes (réseaux sociaux *etc*.) sauf à les bloquer toutes entières ;

– d'autre part, la Commission rappelle qu'il existe des techniques permettant de contourner chaque type de blocage de manière relativement simple : l'utilisation de sites « miroir », c'est-à-dire d'une réplication du site sur une autre adresse *IP*, une autre *url* et un autre nom de domaine, l'utilisation d'un *proxy*, c'est-à-dire d'un site servant d'intermédiaire de connexion entre l'utilisateur et le site auquel il souhaite se connecter, le chiffrement ou le recours à un réseau privé virtuel.

Compte tenu de ces éléments, la Commission estime que le retrait du contenu auprès des hébergeurs doit être privilégié sur le blocage lorsque ces derniers sont coopératifs. À cet égard, elle rappelle que les articles 6-I-2 et 6-I-3 de la LCEN permettent à toute personne, y compris la personne publique, de dénoncer à un hébergeur un contenu manifestement illicite à condition que cette dénonciation soit justifiée dans les conditions prévues par l'article 6-I-5 de la LCEN. L'hébergeur doit alors retirer l'information ou en rendre l'accès impossible sous peine de voir sa responsabilité civile et pénale retenue.

La Commission, consciente que cette solution n'est pas adaptée en présence d'hébergeurs non coopératifs, **recommande l'utilisation du blocage à titre subsidiaire et sur décision judiciaire**.

En outre, dans le cas où un dispositif de blocage serait prévu par la loi, cette dernière doit également prévoir un mécanisme d'évaluation de l'efficacité du dispositif, afin de vérifier que les effets du blocage sont en adéquation avec l'objectif de la restriction et d'éviter tout blocage excessif des contenus.

Recommandation n° 28

N'autoriser le blocage qu'à titre subsidiaire et sur décision judiciaire.

Accompagner tout dispositif de blocage d'un dispositif d'évaluation de son efficacité.

b. Limiter les cas de contournement du juge par les autorités administratives

Dans une démocratie, où le juge est censé être garant de la liberté d'expression et donc seul à pouvoir la limiter, offrir à l'autorité administrative la **possibilité d'ordonner un retrait/blocage/déréférencement sans recours à l'autorité judiciaire** constitue là encore un effet de brèche majeur. Comment justifier en effet la ligne de partage entre les contenus illégaux pour lesquels le blocage administratif est autorisé et les contenus pour lesquels il ne le serait pas ?

Comme on pouvait s'y attendre, des propositions d'étendre le principe du blocage sur décision administrative à d'autres contenus illégaux n'ont pas tardé à fleurir dans le débat public, en s'appuyant légitimement sur le précédent créé. Dans un communiqué de presse du 16 janvier 2015, la garde des Sceaux, Mme Christiane Taubira a ainsi annoncé sa volonté de confier à l'autorité administrative la possibilité de bloquer les sites et messages de haine raciste ou antisémite. Le 30 mars 2015, lors des débats sur la proposition de loi renforçant la lutte contre le système prostitutionnel, les sénateurs ont adopté, contre l'avis du Gouvernement, un amendement tendant à rétablir le dispositif de blocage, sur décision administrative, des sites internet utilisés pour les réseaux de traite et de proxénétisme, dispositif qui avait été supprimé à l'Assemblée nationale. La rapporteure, Mme Michelle Meunier, a estimé que les arguments du Gouvernement (efficacité incertaine et nécessité d'un contrôle du juge judicaire) avaient « *quelque peu perdu de leur portée* » depuis l'adoption de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

La Commission **s'alarme donc du risque de généralisation, de proche en proche, de ce régime d'exception**.

Recommandation n° 29

Ne pas introduire de nouveau cas de blocage sur décision administrative.

De manière générale, la Commission souhaite **mettre en garde le législateur contre la tentation de permettre à des autorités administratives ou à des autorités administratives indépendantes de contourner le juge ou de s'y substituer**.

Cette tentation s'est illustrée avec la création de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet. Dans sa décision n° 2009-580 DC du 10 juin 2009 sur la loi favorisant la diffusion et la protection de la création sur internet (dite « Hadopi 1 »), le Conseil constitutionnel a censuré les dispositions qui tendaient à confier à cette autorité administrative indépendante le pouvoir de couper l'accès à internet de titulaires d'abonnement, en consacrant le droit d'accès à internet comme condition de la liberté d'expression, et en rappelant qu'« *eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins* » [(1)].

Depuis, les propositions de contournement du juge par des autorités administratives ou de substitution d'autorités administratives au juge n'ont cessé de proliférer (voir l'encadré ci-après).

---

(1) Décision n° 2009-580 DC du 10 juin 2009, Loi favorisant la diffusion et la protection de la création sur internet, *considérant 16.*

De nombreuses propositions tendant à contourner le juge par des autorités administratives

Les propositions du Conseil supérieur de l'audiovisuel, évoquées précédemment, d'**étendre à internet les principes de la régulation extra-judiciaire des contenus audiovisuels**, relèvent de cette logique. La Commission les estime dénuées de fondement.

L'avis de la CNCDH sur la lutte contre les discours de haine sur internet du 12 février 2015 propose la création d'une autorité administrative indépendante (AAI) chargée de la « régulation du web » ou l'attribution à une AAI existante (CSA, HADOPI ou CNIL) d'une « *mission de protection des droits et libertés du numérique* ». Cette instance, largement inspirée de l'HADOPI, dont il s'agirait d'adapter le modèle aux « discours de haine sur internet », pourrait notamment procéder à :

« *– un **avertissement de l'usager**, celui-ci **consistant à informer l'internaute de l'infraction commise et des sanctions encourues**. Parallèlement, l'AAI pourrait développer une action de formulation de contre-discours, à l'instar de l'action développée par l'HADOPI en matière de protection du droit d'auteur (…);*

« *– une médiation entre les prestataires privés et les internautes, qu'ils soient auteurs ou victimes d'un contenu illicite. Dans une relation qui s'apparente trop souvent au combat entre David et Goliath, il convient d'apporter une protection à la partie économiquement faible. Il est à ce jour difficile pour l'internaute de faire-valoir ses observations en cas de refus de retrait de contenu illicite, de silence du prestataire privé dûment notifié, ou encore de suppression de contenus considérée comme abusive ;*

« *– la **mise en demeure de l'hébergeur afin qu'il retire un contenu manifestement illicite** ou qu'il republie un contenu licite ;*

« *– la mise en demeure de l'hébergeur aux fins de communiquer les éléments d'identification de l'auteur d'un contenu illicite. En l'absence de réponse du prestataire, l'AAI pourrait saisir le juge en référé* » (1).

L'AAI pourrait également « **ordonner le déréférencement provisoire d'un contenu suspect** ». Elle serait investie d'un pouvoir de sanction et pourrait, « *à la suite d'une mise en demeure infructueuse* » saisir le juge afin qu'il limite l'accès à internet d'un titulaire d'abonnement. Elle pourrait « ***être habilitée à constituer une liste de sites à bloquer** soumise à validation de l'autorité judiciaire, tout en procédant à son actualisation régulière* ».

Le rapport de Mme **Mireille Imbert-Quaretta** de février 2014 sur la lutte contre la contrefaçon en ligne et l'étude annuelle 2014 du **Conseil d'État** proposent également de renforcer les pouvoirs de l'HADOPI en lui confiant la possibilité d'adresser aux sites des « *injonctions de retrait prolongé* » afin d'éviter la réapparition de contenus supprimés après signalement pendant une durée déterminée.

(1) CNCDH, Avis sur la lutte contre les discours de haine sur internet, *12 février 2015, § 32.*

La Commission réaffirme son inquiétude face aux nombreuses propositions qui tendent à affranchir l'espace numérique du contrôle de l'autorité judiciaire et à lui appliquer un régime d'exception en matière de liberté d'expression. Comme indiqué précédemment, elle s'oppose fermement à l'extension à internet du régime extra-judiciaire de régulation de l'audiovisuel et à l'élargissement, proposé par la CNCDH, d'un dispositif calqué sur le « modèle Hadopi » à l'ensemble des contenus de haine.

Recommandation n° 30

Limiter les cas de contournement du juge par des autorités administratives.

3. Renforcer les moyens d'action contre les contenus illégaux dans le respect du rôle du juge

La Commission estime qu'il existe des moyens de renforcer l'efficacité de la lutte contre les contenus illégaux sans remettre en cause les principes de droit protecteurs de la liberté d'expression. S'agissant essentiellement d'actions relevant de politiques publiques, la Commission n'a pas vocation à les examiner dans le détail. Outre l'éducation à la citoyenneté numérique ou le soutien aux contre-discours qui peut s'appuyer sur la force de propagation d'internet, il s'agit évidemment du renforcement des moyens d'action de la justice (**a**), de l'accessibilité et de l'effectivité de la loi de 1881 (***b***) mais aussi de la coopération internationale afin de faciliter la collaboration avec les hébergeurs (***c***) ou de l'amélioration des dispositifs de signalement sur les plateformes (***d***).

a. Renforcer en profondeur les moyens d'action de la justice

La Commission est consciente de ce que la réaffirmation du rôle du juge ne peut se faire sans un renforcement substantiel et une réforme en profondeur de ses moyens d'action visant notamment à obtenir des décisions dans des délais courts. Dans sa recommandation sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, la Commission avait estimé « *possible, et même indispensable, que puisse s'organiser un traitement prioritaire par le parquet des plaintes portant sur des contenus de provocation au terrorisme ou d'apologie du terrorisme. Cette proposition devrait prendre la forme d'une circulaire du garde des Sceaux. La Commission souhaite également que soit évaluée l'opportunité de désigner un juge spécialisé habilité à traiter ces plaintes et/ou d'instaurer la possibilité pour l'autorité administrative de saisir le juge des référés en cas de contenus manifestement odieux (diffusion d'actes de barbarie, meurtres, tortures en ligne, etc.)* » [(1)].

Afin de lutter contre la prolifération de sites miroirs, la Commission a souhaité « *que soit examinée la possibilité de mettre en place une procédure judiciaire accélérée pour les simples réplications de contenus déjà condamnés* » et estimé « *par conséquent qu'une meilleure coordination des services de police et de justice permettrait d'enclencher plus rapidement des procédures contre les contenus visés* ».

La Commission a également souhaité que soit étudié un dispositif inspiré du système de signalement mis en œuvre par l'Autorité de régulation des jeux en ligne (ARJEL), qui permettrait à l'autorité administrative de présenter à dates

---

(1) Voir la recommandation du 22 juillet 2014 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme.

régulières à l'autorité judiciaire des séries de contenus à bloquer. Cette solution permettrait à la France de rester cohérente par rapport aux principes qu'elle défend à l'étranger en matière de droits de l'homme, et notamment le principe que « *toute législation visant à restreindre le droit à la liberté d'opinion ou d'expression doit être appliquée par une entité indépendante de toute influence politique, commerciale ou autre d'une manière qui ne soit ni arbitraire ni discriminatoire et avec assez de garde-fous pour la mettre à l'abri de l'abus ; elle doit prévoir des voies de recours et de réparation contre son application abusive* » (1).

Elle retient également les propositions du Conseil national du numérique de « *spécialiser la chaîne pénale en matière de blocage DNS judiciaire des sites et de retrait de contenus pour une action plus rapide et efficace* :

– *créer un parquet spécialisé, sur les questions de contenus illicites en ligne, notamment par la mise en place de magistrats référents au sein des parquets et réseaux d'experts. La France s'est dotée fin 2013 de moyens renforcés en matière de délinquance financière (création d'un parquet financier dédié). Une démarche similaire serait plus que souhaitable en matière de lutte contre les contenus illicites sur Internet ;*

– *créer un « pôle de compétences numériques » au sein du ministère de la Justice dédié à la mise en œuvre d'une politique pénale en la matière et au suivi des travaux européens et internationaux relatifs à la criminalité en ligne. Ce service pourrait aussi avoir un rôle d'expertise et de conseil auprès des magistrats en poste en juridiction ;*

– *créer une filière de formation* ad hoc *des juges au numérique : créer des modules spécifiques dans les formations initiale et continue* ».

Elle estime également, comme le Conseil, qu'il convient de « *réinvestir et capitaliser sur les procédures existantes, trop souvent écartées : en particulier les procédures d'urgence et le référé LCEN* » (2).

---

(1) Orientations du Conseil de l'Union Européenne relatives à la liberté d'expression en ligne et hors ligne, 12 mai 2014, § 22.

(2) Conseil national du numérique, op. cit., *pp. 82-83.*

Recommandations nos 31 à 37

– n° 31 : organiser un traitement prioritaire par le parquet des plaintes portant sur des contenus particulièrement odieux (en particulier les contenus d'apologie du terrorisme et de provocation au terrorisme) ;

– n° 32 : évaluer l'opportunité de désigner un juge spécialisé, au besoin de proximité, habilité à traiter ces plaintes et/ou instaurer la possibilité pour l'autorité administrative de saisir le juge des référés en cas de contenus manifestement odieux (diffusion d'actes de barbarie, meurtres, tortures en ligne, etc.) ;

– n° 33 : examiner la possibilité de mettre en place une procédure judiciaire accélérée pour les simples réplications de contenus déjà condamnés ;

– n° 34 : mettre à l'étude un dispositif inspiré du système de signalement mis en œuvre par l'Autorité de régulation des jeux en ligne (ARJEL), qui permettrait à l'autorité administrative de présenter à dates régulières à l'autorité judiciaire des séries de contenus particulièrement odieux à bloquer ;

– n° 35 : créer un parquet spécialisé sur les questions de contenus illicites en ligne ;

– n° 36 : créer un « pôle de compétences numériques » au sein du ministère de la Justice dédié à la mise en œuvre d'une politique pénale en la matière et au suivi des travaux européens et internationaux relatifs à la criminalité en ligne. Ce service pourrait aussi avoir un rôle d'expertise et de conseil auprès des magistrats en poste en juridiction ;

– n° 37 : créer une filière de formation ad hoc des juges au numérique : créer des modules spécifiques dans les formations initiale et continue.

b. Renforcer l'accessibilité et l'effectivité de la loi de 1881

La CNCDH, dans son avis précité sur la lutte contre les discours de haine, formule plusieurs propositions destinées à améliorer l'effectivité de la loi de 1881 que la Commission juge très pertinentes. Il s'agit notamment d'améliorer la clarté et la lisibilité des dispositions de la loi de 1881 en précisant et en actualisant les notions d'espace public et d'espace privé, au regard des nouvelles formes de communautés et de réseaux du *web 2.0*, d'envisager la numérisation des procédures et de prévoir un droit de réponse effectif sur internet au profit des associations antiracistes.

Recommandation n° 38

Améliorer l'effectivité de la loi de 1881 sur la liberté de la presse :

– préciser et actualiser les notions d'espace public et d'espace privé, au regard des nouvelles formes de communautés et de réseaux numériques du *web 2.0* ;

– envisager la numérisation des procédures, notamment des assignations et significations ; simplifier et faciliter les procédures de référé par la création d'un référé numérique et prévoir la possibilité de déposer plainte en ligne ;

– prévoir un droit de réponse effectif sur internet au profit des associations antiracistes.

c. Garantir les conditions d'une meilleure coopération des hébergeurs

Dans son étude annuelle 2014, le Conseil d'État propose de définir un socle de règles jouant un rôle particulièrement important dans la protection des droits fondamentaux, qui seraient applicables à tous les acteurs dirigeant leurs services vers la France ou l'Union européenne, quel que soit leur lieu d'établissement. Seraient notamment concernés l'obligation de coopération des hébergeurs avec les autorités administratives et judiciaires et le droit pénal, notamment les abus de la liberté d'expression.

En effet, les II et II *bis* de l'article 6 de la LCEN, qui prévoient les obligations de conservation des données et de coopération avec les autorités judiciaires et administratives applicables aux hébergeurs, ne définissent pas leur champ d'application territorial. La loi devrait donc **prévoir que l'obligation de coopération est applicable à tout hébergeur dirigeant ses activités vers la France**.

La Commission appelle aussi, comme le Conseil national du numérique, à :

« *– réformer le MLAT (*Mutual Legal Assistance Treaty*) entre la France et les États-Unis, qui permet à l'autorité judiciaire française d'accéder à des informations stockées dans des plateformes hébergées aux États-Unis, visant à une plus grande rapidité dans l'échange des données ;*

– entreprendre une action diplomatique forte pour faire signer et ratifier par les États hébergeant des sites diffusant des discours de haine le protocole additionnel n° 189 à la Convention cybercriminalité du Conseil de l'Europe spécifiquement dédié au racisme et à l'antisémitisme » [(1)].

---

(1) Conseil national du numérique, op. cit.*, p. 80.*

Recommandations n°s 39 à 41

– n° 39 : prévoir l'application à tout hébergeur dirigeant ses activités vers la France des obligations de coopération avec les autorités administratives et judiciaires prévues par l'article 6 de la LCEN ;

– n° 40 : réformer le MLAT (*Mutual Legal Assistance Treaty*) qui permet à l'autorité judiciaire française d'accéder à des informations stockées dans des plateformes hébergées aux États-Unis dans le but de favoriser une plus grande rapidité dans l'échange des données ;

– n° 41 : entreprendre une action diplomatique forte pour faire signer et ratifier par les États hébergeant des sites diffusant des discours de haine le protocole additionnel n° 189 à la Convention cybercriminalité du Conseil de l'Europe spécifiquement dédié au racisme et à l'antisémitisme.

d. Renforcer les dispositifs de signalement sur les plateformes

Compte tenu de l'intérêt général attaché à la répression de certains contenus particulièrement odieux, l'article 6-I-7 de la LCEN oblige les FAI et hébergeurs à mettre en place un dispositif facilement accessible et visible permettant à toute personne de leur signaler ce type de contenu, à informer promptement les autorités publiques compétentes en cas de signalement et à rendre publics les moyens qu'ils consacrent à la lutte contre ces activités illicites.

En ce qui concerne la mise en œuvre de cette obligation, le rapport de Marc Robert de février 2014 sur la lutte contre la cybercriminalité observe des pratiques hétérogènes selon les prestataires. « *Ainsi les prestataires membres de l'Association des fournisseurs d'accès à Internet (AFA) ont-ils mobilisé leur service de signalement "*Pointdecontact*". Les pratiques des prestataires non membres de l'AFA varient : si Facebook comme* Twitter *ont mis en place un dispositif de base suite aux pressions ministérielles, en revanche, d'autres prestataires, notamment français tels que* Free*, refusent toujours de se soumettre à une telle obligation. Enfin, l'accessibilité et la visibilité du dispositif sont souvent sujettes à caution* » [(1)].

La Commission appelle à une simplification et à une standardisation des différents dispositifs de signalement et de notification qui se développent à ce jour de manière totalement désordonnée.

Le Conseil national du numérique formule également plusieurs propositions intéressantes en particulier :

« *– renforcer et généraliser les dispositifs de* fast track *accordés aux associations. Certaines associations de lutte contre les discriminations disposent*

---

(1) Groupe de travail interministériel sur la lutte contre la cybercriminalité, Protéger les internautes. Rapport sur la cybercriminalité, *février 2014, p. 186.*

d'un accès privilégié aux outils de signalement. Il s'agit de généraliser ces procédures ;

– obtenir des obligations de traitement dans des délais donnés pour les signalements opérés par les internautes auprès des plateformes ;

– et donner plus de visibilité à la plateforme PHAROS auprès des particuliers, notamment dans les interfaces des plateformes » [(1)].

Enfin, la Commission recommande l'augmentation des moyens humains, techniques et matériels de la plateforme de signalement PHAROS.

Recommandations n°s 42 à 46

– n° 42 : organiser la simplification et la standardisation des différents dispositifs de signalement et de notification développés par les plateformes de manière totalement désordonnée ;

– n° 43 : renforcer et généraliser les dispositifs de *fast track* accordés aux associations ;

– n° 44 : obtenir des obligations de traitement dans des délais donnés pour les signalements opérés par les internautes auprès des plateformes ;

– n° 45 : donner plus de visibilité à la plateforme PHAROS auprès des particuliers, notamment dans les interfaces des plateformes ;

– n° 46 : augmenter les moyens humains, techniques et matériels de la plateforme de signalement PHAROS.

(1) Conseil national du numérique, op. cit., *p. 84.*

III. REPENSER LA PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES À CARACTÈRE PERSONNEL

La société et l'économie numériques ont connu, ces dernières années, de profonds bouleversements affectant la manière dont la vie privée est exposée et protégée ainsi que les modalités de collecte et d'utilisation des données à caractère personnel. De nombreuses mutations, à la fois techniques, économiques, sociales et culturelles, caractérisent cette dimension de la « révolution numérique ». La Commission se bornera ici à rappeler les traits saillants de ces nouvelles pratiques [(1)] :

– sur le plan technique, l'on assiste à une « mise en données » ou « datification » du monde permise par la progression exponentielle des moyens de captation, de stockage, de reproduction et d'analyse des données, l'explosion du volume des données qui transitent par eux (mégadonnées ou *big data*) et l'essor de l'internet des objets et de l'intelligence artificielle ;

– au niveau économique, certains secteurs d'activité ont vu leur modèle de croissance profondément transformé par une logique de valorisation intensive des données personnelles disponibles, permettant notamment un ciblage publicitaire fin des consommateurs sous la forme de publicités contextuelles, personnalisées ou comportementales, et la production de services personnalisés, plus performants ou simplement nouveaux ;

– les implications sociales et culturelles de ces mutations se mesurent à l'adoption rapide des usages fixes et mobiles d'internet sur différents supports, grâce à la multiplication des pratiques de partage d'informations, d'expressions, d'opinions ou de publication de documents personnels sur des plateformes dédiées ou sur les réseaux sociaux.

Ces bouleversements ont redéfini la conception de la vie privée et transformé la valeur attachée à sa protection ainsi qu'à celle des données à caractère personnel.

Comme l'a indiqué devant la Commission le 26 novembre 2014 Mme Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL), « *notre époque se caractérise par une imprégnation des données personnelles dans toutes les activités publiques, professionnelles ou privées. L'individu est de plus en plus pris dans un maillage extrêmement fin d'informations personnelles relayées par des objets de plus en plus communicants : téléphone portable, bracelets électroniques divers, dispositifs électriques, équipements de vidéosurveillance, etc. Cette " datification " (...) du monde (...) illustre (...) l'entrée dans un numérique ambiant* » dans lequel « *la dichotomie qui existait encore il y a quelques années entre les univers physique et virtuel (...) a disparu* ». Cette imprégnation « *change le rapport qui existait entre*

---

(1) Pour plus de précisions, voir notamment : Conseil d'État, op. cit., *pp. 41-69 et rapport d'information (n° 3560, XIIIe législature) de MM. Patrick Bloche et Patrice Verchère au nom de la mission d'information commune sur les droits de l'individu dans la révolution numérique, juin 2011, pp. 123-149.*

vie privée et données personnelles. Jusqu'à une période récente, les protections de ces deux sphères se superposaient. Sous l'effet des nouveaux comportements et usages, la frontière entre la vie privée et la vie publique commence à se détendre pour donner naissance à une zone un peu grise dans laquelle les personnes veulent exposer leur vie privée et se servent des données personnelles pour avoir une vie publique » et, tout en demandant une protection, « *recherchent avant tout une maîtrise* ».

Pour certains, il existerait même une forme de « *paradoxe de la vie privée* » (*privacy paradox* [(1)]) selon lequel, dans l'environnement numérique, propice à la théâtralisation, à l'exposition et à la publicisation de soi (*publicness* [(2)]), les individus, convaincus que les technologies numériques participent à la construction de leur personnalité et à leur valorisation sociale et professionnelle, mettraient eux-mêmes en danger leur vie privée en échange de services ou d'avantages, sans toutefois renoncer à un haut niveau de protection et de maîtrise sur leurs données personnelles (voir l'encadré ci-après).

L'importance variable accordée à la protection de la vie privée

De nombreuses études en psychologie et en économie comportementale ont démontré la valeur très variable, contextuelle et parfois peu rationnelle que les individus tendent à accorder à la protection de leurs données personnelles :

– une étude menée aux États-Unis et à Singapour montre que la protection des données personnelles contre les erreurs, les accès non autorisés ou les usages détournés (non conformes aux finalités) serait valorisée entre 30 et 45 dollars par les internautes ; cependant, une différence de 2 dollars sur une carte d'achat peut sembler suffisante à une majorité de détenteurs pour compenser une perte d'anonymat dans des transactions en ligne [(1)] ;

– les consommateurs bénéficiant de mécanismes de contrôle de leurs données sur une plateforme numérique se montreraient plus enclins à communiquer des données sensibles, en raison de la diminution du degré de vigilance suscitée par l'accroissement des moyens de contrôle qui leur sont donnés [(2)] ;

– les internautes ne liraient pas les conditions générales d'utilisation qu'ils acceptent [(3)] puisque, au terme d'une expérimentation, 7 500 personnes avaient accepté de céder leur âme pour l'éternité à un fournisseur de services.

(1) Alessandro Acquisti, Laura Brandimarte, George Loewenstein, « Privacy and human behavior in the age of information », Science *30 January 2015, vol. 345, n° 6221, pp. 509-514.*

(2) Laura Brandimarte, Alessandro Acquisti et George Loewenstein, « Misplaced Confidences: Privacy and the Control Paradox », 2010.

(3) Frederik J. Zuiderveen Borgesius, « Consent to behavioural targeting in european law - What are the policy implications of insights from behavioural economics ? », 2013.

Pour d'autres, loin d'être devenu une « *anomalie* » [(3)] ou d'avoir totalement disparu, le droit au respect de la vie privée se serait transformé pour

---

(1) Notion notamment développée par Mme Susan B. Barnes.

(2) Notion forgée par M. Jeff Jarvis dans J. Jarvis, Public parts : How sharing in the digital age improves the way we work and live, *Simon & Schuster, 2011.*

(3) Pour M. Eric Schmidt, alors président-directeur général de Google, *auditionnée par la* Federal Trade Commission *en novembre 2013.*

passer, selon M. Antonio Casilli, d'un droit individuel à être laissé en paix et protégé des intrusions d'autrui à une négociation collective destinée à maîtriser la projection de soi dans les interactions sociales avec autrui [(1)].

Dans ce nouveau contexte, la Commission s'est interrogée sur l'adéquation de notre cadre juridique avec les nouvelles réalités posées par le numérique et ses développements récents. À cette fin, elle a procédé à plusieurs auditions et constitué, en son sein, un groupe de travail chargé de réfléchir à la notion de vie privée.

De prime abord, elle estime que **les principes généraux posés par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et libertés », et 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, transposée en droit interne en 2004 [(2)], demeurent fondés et pertinents**. Pour la Commission, il serait pour le moins paradoxal de vouloir les remettre en cause aujourd'hui alors que c'est précisément leur nature et leur étendue qui ont permis à notre législation de connaître une remarquable stabilité depuis 1978. Son approche transversale a en effet permis de couvrir un large spectre de données personnelles et de traitements :

– en reconnaissant à l'individu des droits face aux responsables de traitements : droit à l'information sur l'utilisation des données collectées, sauf pour les traitements intéressant la sûreté de l'État ou la sécurité publique [(3)], droit d'opposition pour des motifs légitimes, sauf si le traitement répond à une obligation légale, y compris face à l'utilisation des données à des fins de prospection [(4)], droits d'accès ou de rectification [(5)], droit de connaître et de contester les informations et résultats utilisés dans les traitements automatisés, interdiction, absolue ou relative, de fonder une décision de justice ou toute autre décision impliquant une appréciation sur le comportement d'un individu sur un traitement de données [(6)] ;

– en permettant une application des normes adaptée aux cas d'espèce et évolutive, grâce au rôle qu'elle a confié à un régulateur indépendant, en France la CNIL ;

---

(1) Antonio Casilli, « Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée », in Conseil d'État, op. cit., *pp. 423-434.*

(2) Par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(3) Article 32 de la loi n° 78-17 du 6 janvier 1978 précitée et articles 10 et 11 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(4) Article 38 de la loi n° 78-17 du 6 janvier 1978 précitée et articles 14 et 15 de la directive 95/46/CE du 24 octobre 1995 précitée.

(5) Articles 39 à 43 de la loi n° 78-17 du 6 janvier 1978 précitée et article 12 de la directive 95/46/CE du 24 octobre 1995 précitée.

(6) Article 10 de la loi n° 78-17 du 6 janvier 1978 précitée.

– en posant des exigences de proportionnalité et de limitation toujours d'actualité : obligations de loyauté [1], de collecte pour des finalités déterminées, explicites et légitimes [2], proportionnalité de la collecte aux finalités [3], exactitude des données [4], limitation de la durée de conservation [5] et sécurité des données [6].

Certains de ces principes ont pu paraître dépassés à l'ère du *big data*, fondé, par définition, sur la collecte du plus grand nombre de données possible – en contradiction avec les principes de finalités déterminées, de proportionnalité et d'exactitude – et des durées de conservation les plus longues possible – en contradiction avec le principe de limitation de la durée de conservation. Ces principes, essentiels à la confiance des personnes dans la société numérique, doivent toutefois être conservés. Au surplus, ils n'interdisent pas de tenir compte des spécificités des usages du *big data* à caractère statistique, en ne soumettant la conservation des données collectées à cette fin à aucune limitation de durée et en permettant leur réutilisation à d'autres fins que celles qui ont justifié leur collecte [7].

Derrière ce constat général, force est toutefois d'admettre que le cadre juridique applicable aux traitements de données personnelles ne s'est pas pleinement adapté aux nouvelles réalités numériques. Ces dernières exigent de repenser la protection de la vie privée et des données à caractère personnel, conçue à une époque où les techniques de collecte et d'exploitation à la disposition des acteurs privés et étatiques n'étaient pas aussi nombreuses et perfectionnées qu'aujourd'hui. Les usagers des réseaux numériques eux-mêmes formulent de nouvelles exigences parfois contradictoires, en souhaitant à la fois davantage de protection mais aussi une plus grande autonomie dans la gestion et dans la maîtrise de leurs données.

---

(1) 1° de l'article 6 de la loi n° 78-17 du 6 janvier 1978 précitée.

(2) 2° du même article.

(3) 3° du même article.

(4) 4° du même article.

(5) 5° du même article.

(6) Article 34 de la loi n° 78-17 du 6 janvier 1978 précitée.

(7) L'article 6 de la loi n° 78-17 du 6 janvier 1978 précitée prévoit qu'un traitement ultérieur des données à des fins statistiques est considéré comme compatible avec les finalités initiales du traitement à condition de respecter les procédures de déclaration du traitement statistique auprès de la CNIL et les obligations d'information des personnes concernées et de sécurité des données. L'article 8 de la même loi permet de déroger à l'interdiction de collecter et de traiter des données sensibles pour les traitements réalisés par les services de la statistique publique dans le cadre de la loi du 7 juin 1951 sur l'obligation, la coordination et le secret en matière statistique, après autorisation de la CNIL (de manière générale, le traitement de données sensibles peut être autorisé par la CNIL si ces données vont faire l'objet à bref délai d'une anonymisation reconnue conforme par la CNIL). L'article 10 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal dispose que les informations publiques « peuvent être utilisées par toute personne qui le souhaite à d'autres fins que la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus *», l'article 13 de la même loi prévoyant que lorsque ces informations comportent des données à caractère personnel, leur réutilisation est possible à d'autres fins à condition que les personnes concernées aient donné leur consentement, que la personne détentrice soit en mesure de les anonymiser ou qu'une disposition législative l'autorise.*

Dans ces conditions, la Commission a souhaité formuler plusieurs recommandations, toutes inspirées par une même conviction partagée par l'ensemble de ses membres : **diversifier l'approche traditionnelle qui a inspiré notre législation, fondée sur l'exigence de protection des individus face aux risques soulevés par les traitements de données personnelles, au profit d'un renforcement de leurs capacités d'agir et de la maîtrise de leurs données**. Car la vie privée doit aujourd'hui être conçue tout à la fois comme une zone de protection et une zone de liberté ; elle est, pour reprendre les mots du professeur Jean Rivero, « *cette sphère de chaque existence dans laquelle nul ne peut s'immiscer sans y être convié. La liberté de la vie privée est la reconnaissance, au profit de chacun, d'une zone d'activité qui lui est propre et qu'il est maître d'interdire à autrui* » [(1)].

Les premières recommandations de la Commission, transversales, ont vocation à adapter le cadre juridique en vigueur à l'utilisation du numérique par les acteurs privés et publics afin de renforcer l'effectivité des droits au respect de la vie privée et à la protection des données à caractère personnel (**A**). Certaines, plus sectorielles, visent à donner davantage d'autonomie à l'individu dans l'univers numérique face aux pratiques de sociétés commerciales qui collectent, exploitent et conservent leurs données à grande échelle (**B**). D'autres enfin tendent à restaurer un véritable droit à la protection de la vie privée et des données personnelles face aux activités régaliennes (**C**).

A. RÉÉVALUER L'IMPORTANCE DES DROITS AU RESPECT DE LA VIE PRIVÉE ET À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Il est apparu nécessaire de procéder à une triple réévaluation de l'importance conférée au respect de la vie privée et à la protection des données à caractère personnel dans l'univers numérique par la consécration explicite de ces droits au niveau constitutionnel (**1**), l'élargissement du champ couvert par la notion de « donnée à caractère personnel » (**2**) et l'adaptation du mode de régulation des responsables de traitements (**3**).

1. Faire des droits au respect de la vie privée et à la protection des données personnelles des droits fondamentaux constitutionnellement garantis

Face à la massification et à la diversification de la collecte et des usages des données personnelles (***a***), la Commission invite à pallier l'absence paradoxale de consécration au plus haut niveau de la hiérarchie des normes des droits au respect de la vie privée et à la protection des données à caractère personnel (***b***) par leur inscription dans la Constitution (***c***).

---

(1) Jean Rivero, Libertés publiques, *Montchrestien, 1989, p. 74.*

a. La massification de la collecte et la diversification des usages des données à caractère personnel

L'exposition, volontaire ou subie, de la vie privée des individus a pris, à l'ère numérique, une ampleur inédite, avec l'essor des pratiques de collecte et d'exploitation d'informations personnelles de toutes sortes (informations confidentielles, données à caractère personnel, traces, etc.) et à des fins diverses, qu'il s'agisse de finalités commerciales ou de protection de l'ordre public.

Un nombre croissant d'acteurs puissants qui fournissent des services aux consommateurs, singulièrement les opérateurs de télécommunications, les moteurs de recherche et les réseaux sociaux, ont accès à une multitude de données à caractère personnel. Aux données recueillies aux fins de constitution de fichiers sur les individus, source historique de notre législation sur l'encadrement des traitements de données à caractère personnel, il faut aujourd'hui ajouter les données mises en ligne par les individus eux-mêmes sur les réseaux sociaux ou les sites de partage, portant sur leur propre vie ou sur celle de tierces personnes, et les données recueillies automatiquement, par exemple sous la forme de *cookies* ou de signaux de localisation [(1)]. En effet, avec la géolocalisation, une économie cachée de la collecte d'identifiants et de traces permet de suivre, d'analyser, de mesurer et de monétiser l'activité et les usages des utilisateurs d'appareils mobiles, notamment à des fins commerciales et publicitaires. Diverses, ces données sont de surcroît extrêmement hétérogènes par leur nature, allant des caractéristiques objectives de la personne à des informations plus personnelles et subjectives, comme ses goûts, ses opinions ou ses relations.

Cette collecte massive de données est désignée sous le nom de mégadonnées (*big data*), communément caractérisée par la formule des « trois V » pour *volume*, *variété* et *vélocité*, eu égard à la masse des données collectées, à leur grande diversité et à la rapidité de leur traitement permise par les nouvelles générations de technologies et d'algorithmes qui décuplent les possibilités d'analyse et de calcul (ciblage publicitaire, aide au diagnostic médical, veille sanitaire, prévention du déclenchement de phénomènes naturels, développement de « villes intelligentes », etc.) [(2)]. Cette collecte massive de données personnelles est facilitée, voire amplifiée, par « l'infrastructure » de l'économie numérique, animée par des logiques de rachat et de fusion de sociétés [(3)] et l'essor de courtiers en données personnelles (*data brokers*) spécialisés dans la revente des données collectées [(4)].

Ainsi que l'ont démontré plusieurs chercheurs, la puissance de calcul et d'analyse permise par le *big data*, combinée aux capacités de stockage offertes par l'informatique en nuage (*cloud computing*) et l'extrême diversité des données

---

(1) Conseil d'État, op. cit., *pp. 16-17.*

(2) CNIL, Rapport d'activité 2012, *« Big data, tous calculés ? », p. 80.*

(3) Par exemple, rachat par Facebook *des sites de partage de photographies* Instagram *et de messagerie instantanée* Whatsapp.

(4) Ainsi la société Acxiom *affirme-t-elle détenir des données sur 700 millions de personnes dans le monde.*

recueillies ou partagées font naître des systèmes de détection, de classification et d'évaluation anticipative des comportements humains, appelés par Mme Antoinette Rouvroy notamment, « *gouvernementalité algorithmique* » [(1)]. Cette nouvelle gouvernementalité numérique conduit à des prises de décision automatique ou semi-automatique, anticipant les comportements, les goûts et les choix de chacun, grâce au *data mining* et aux techniques de profilage qui permettent d'individualiser les offres de services sans se préoccuper des intentions ni recueillir les préférences des personnes concernées.

b. Des normes constitutionnelles paradoxalement silencieuses

Or le cadre normatif applicable en France et en Europe à la collecte et aux usages des données personnelles a été pensé à une époque où les réseaux numériques n'étaient ni utilisés ni appréhendés par les individus de la même manière qu'aujourd'hui. Il est particulièrement frappant de constater que les normes constitutionnelles qui protègent les droits et libertés fondamentaux des individus ne mentionnent nulle part le droit de chacun au respect de sa vie privée et à la protection de ses données personnelles. Ces droits ne sont inscrits ni dans la Constitution du 4 octobre 1958, ni dans son préambule.

Il est vrai que certaines dispositions de nature législative protègent ces droits. La loi du 17 juillet 1970 a ainsi inséré un article 9 au sein du code civil qui dispose, en son premier alinéa, que « *chacun a droit au respect de sa vie privée* ». D'autres dispositions, de nature pénale, répriment les violations de l'intimité de la vie privée, notamment les articles 226-1, 226-2, 226-3, 226-4-1 ou 226-22 du code pénal. Mais c'est par le seul effet de la jurisprudence développée par le Conseil constitutionnel que ces droits ont été progressivement et partiellement reconnus. Ce dernier a ainsi jugé, dans une décision du 23 juillet 1999 [(2)] confirmée par la suite [(3)], que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 « *implique le respect de la vie privée* », principe qui figure au nombre des droits et libertés constitutionnellement garantis dont la mise en œuvre incombe à la fois au juge judiciaire et au juge administratif. Le Conseil constitutionnel n'a tiré que très récemment les conséquences de ce droit en matière de protection des données personnelles, en jugeant à partir de 2012 que « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un*

---

(1) Antoinette Rouvroy et Thomas Berns, « Le nouveau pouvoir statistique », Multitudes *n° 40, pp. 88-103, 2010 ; CNIL,* Cahiers Innovation et prospective n° 1, *« La "dictature" des algorithmes : demain, tous calculés ? », pp. 18-20.*

(2) Décision n° 99-416 du 23 juillet 1999, Loi portant création d'une couverture maladie universelle, *considérant 45.*

(3) Voir par exemple les décisions du Conseil constitutionnel portant sur le traitement de données à caractère personnel au sein de fichiers de police (décision n° 2003-467 DC du 13 mars 2003, Loi relative à la sécurité intérieure, *considérants 17 à 46 ; décision n° 2010-25 QPC du 16 septembre 2010 ; décision n° 2011-625 DC du 10 mars 2011,* Loi d'orientation et de programmation pour la performance de la sécurité intérieure, *considérants 9 à 13).*

motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif » [(1)].

Cette situation, qui démontre la relative obsolescence et l'inadaptation de notre *corpus* constitutionnel aux réalités de la société numérique, tranche également avec la reconnaissance dont ces droits ont fait l'objet en droit international.

Le principe du respect de la vie privée est explicitement affirmé et protégé par plusieurs instruments internationaux, parmi lesquels la Déclaration universelle des droits de l'homme du 10 décembre 1948 [(2)], le Pacte international relatif aux droits civils et politiques du 16 novembre 1966 [(3)], entré en vigueur le 23 mars 1976 et ratifié par la France le 4 novembre 1966 et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CESDH) du 4 novembre 1950 [(4)], ratifiée par la France le 3 mai 1974 et interprétée par la Cour européenne des droits de l'Homme (CEDH) qui considère qu'elle « *assure à l'individu un domaine dans lequel il peut poursuivre librement le développement et l'accomplissement de sa personnalité* » [(5)].

Le droit à la protection des données à caractère personnel est explicitement consacré par certaines normes internationales, comme la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [(6)], dite « 108 ». Fait notable, il est, depuis 2007, un droit fondamental dans l'ordre juridique de l'Union européenne, distinct du droit au respect de la vie privée. L'article 8 de la Charte européenne des droits fondamentaux de l'Union européenne du 7 décembre 2000 [(7)], à laquelle le traité de Lisbonne du 13 décembre 2007 [(8)] a conféré valeur juridique contraignante, prévoit ainsi, distinctement de son article 7 relatif au respect de la vie privée, que les données à caractère personnel « *doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de*

---

(1) Décisions n°s 2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité, *considérant 8, et 2014-690 DC du 13 mars 2014,* Loi relative à la consommation, *considérant 57.*

(2) Son article 12 dispose que « nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation *» et que «* toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

(3) Son article 17.1 prévoit que « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ».

(4) Aux termes de son article 8, « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

(5) CEDH, 12 juillet 1977, Bruggemann et Scheuten c. RFA, *n° 6959/75.*

(6) Son article 1er protège le « droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données ») ».

(7) Charte européenne des droits fondamentaux de l'Union européenne du 7 décembre 2000 (2010/C 83/02).

(8) Traité de Lisbonne modifiant le traité sur l'union européenne et le traité instituant la communauté européenne (2007/C 306/01).

la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi », que « *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* ». Enfin, si la CESDH ne comporte pas d'article spécifiquement consacré à la protection des données personnelles, la CEDH protège expressément ce droit sur le fondement du droit au respect de la vie privée mentionné par l'article 8 de la Convention en jugeant que « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale* » (1).

c. Vers une constitutionnalisation des droits au respect de la vie privée et à la protection des données à caractère personnel ?

Le besoin qu'a eu le Conseil constitutionnel de dégager de principes constitutionnels anciens le droit au respect de la vie privée et d'en déduire l'exigence de protection des données personnelles témoigne à lui seul de la nécessité de les expliciter à l'avenir davantage dans la Constitution ou les normes qui lui sont rattachées.

Par ailleurs, la protection internationalement reconnue à ces droits n'est pas exclusive de leur consécration constitutionnelle en France, sauf à se satisfaire d'une garantie « inférieure » ou « implicite » de ces valeurs en droit interne.

Au surplus, ainsi que l'ont observé de nombreuses personnes entendues par la Commission, les conditions actuelles de collecte, d'exploitation et de conservation des données à caractère personnel ne permettent plus de considérer le droit à la protection des données personnelles comme une simple déclinaison du droit au respect de la vie privée. Pour Mme Isabelle Falque-Pierrotin, présidente de la CNIL, auditionnée le 26 novembre 2014, si « *certains rétorquent que la protection constitutionnelle de la vie privée existe déjà et qu'il est inutile d'y ajouter celle des données personnelles* », cet argument « *n'est plus exact car ces deux sphères s'autonomisent de manière croissante* » et ne sont pas mises en cause de la même manière selon la nature, l'étendue et l'objet du traitement ou du fichier considéré. Les données personnelles sont devenues l'une des composantes à part entière de l'identité et de la personnalité des individus, qui méritent d'être protégées comme telles même lorsqu'elles ne touchent pas au cœur de l'intimité de leur vie privée.

Pour autant, la Commission n'est pas unanime à l'idée de consacrer dès maintenant ces nouveaux droits dans la Constitution. Certains membres appellent, au préalable, à un encadrement législatif communautaire plus précis et contraignant sur ce sujet, afin d'éviter toute distorsion de concurrence entre pays européens dans le développement de nouveaux modèles économiques. Ces membres estiment du devoir de la France de porter cette ambition au niveau européen.

---

(1) CEDH, 4 décembre 2008, S. et Marper c. Royaume-Uni, *n°s 30562/04 et 305566/04.*

Toutefois, une majorité des membres de la Commission propose de **consacrer explicitement et séparément dans la Constitution du 4 octobre 1958 les droits, d'une part, au respect de la vie privée, et, d'autre part, à la protection des données à caractère personnel**. La définition du **droit au respect de la vie privée** pourrait s'inspirer de la conception qu'en a développé jusqu'à ce jour le Conseil constitutionnel et la définition qu'en ont donnée les normes et les juridictions communautaires et européennes. Une telle consécration permettrait, pour ce qui concerne son volet numérique, de mieux protéger notamment le **droit au secret des correspondances numériques** et le **droit à l'inviolabilité du domicile numérique** face à certaines technologies intrusives [(1)].

La définition du **droit à la protection des données personnelles** pourrait pour sa part reprendre celle qu'en a donné l'article 8 de la Charte européenne des droits fondamentaux de l'Union européenne, en parfaite cohérence avec les exigences posées par le droit communautaire dans ce domaine. Sa consécration permettrait d'élever les conditions d'exploitation des données personnelles à l'ère numérique en **soumettant leur traitement à l'exigence de loyauté et à l'existence de fins déterminées ainsi que d'un fondement légitime ou du consentement de l'intéressé**. Elle devrait également **protéger à un haut niveau le droit pour la personne concernée à accéder aux données collectées qui la concernent et le droit d'en obtenir la rectification au sens large**. Elle devrait enfin garantir le **contrôle du respect de ces règles par une autorité indépendante et impartiale**.

Une telle consécration présenterait plusieurs avantages. Tout d'abord, ainsi consacrés, ces droits se verraient érigés en exigences constitutionnelles de valeur équivalente à d'autres, comme la liberté d'entreprendre ou la liberté d'expression respectivement protégées par les articles 4 et 11 de la Déclaration des droits de l'homme et du citoyen de 1789, rendant plus aisée leur conciliation.

Par ailleurs, une telle consécration permettrait, comme l'a noté au cours de son audition Mme Isabelle Falque-Pierrotin, « *d'afficher une protection du plus haut niveau dans ce domaine, ce qui serait très utile lors des négociations internationales* » engagées au niveau de l'Union européenne et avec d'autres pays comme les États-Unis.

Enfin, elle rapprocherait la France des treize autres pays européens qui ont également procédé à la constitutionnalisation spécifique du droit à la protection des données à caractère personnel, en particulier l'Allemagne, l'Autriche, l'Espagne, la Grèce, la Hongrie, les Pays-Bas, le Portugal ou la Suède [(2)]. Pour ne prendre que quelques exemples, l'article 9 A de la Constitution grecque dispose que « *chaque individu a le droit d'être protégé contre la collecte, le traitement et l'utilisation, en particulier par voie électronique, de ses données personnelles,*

---

(1) Voir infra, *le* b *du* 1 *du C du présent III.*

(2) Rapport d'information (n° 441, session ordinaire de 2008-2009) de M. Yves Détraigne et Mme Anne-Marie Escoffier au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, mai 2009, pp. 16-17.

selon des conditions prévues par la loi. La protection des données personnelles est assurée par une autorité indépendante, qui est constituée et fonctionne selon des conditions prévues par la loi ». En Espagne, l'arrêt 292-2000 du Tribunal constitutionnel, s'inspirant des travaux préparatoires de la Charte européenne des droits fondamentaux, a également reconnu explicitement le droit fondamental à la protection des données à caractère personnel comme un droit autonome et distinct du droit au respect de la vie privée [(1)].

Recommandation n° 47 *(pas d'unanimité)*

Inscrire explicitement dans la Constitution le droit au respect de la vie privée et l'exigence de protection des données à caractère personnel afin de réévaluer l'importance accordée à ces libertés fondamentales en droit interne.

2. Retenir une conception extensive des informations personnelles protégées par ce droit

Corrélativement, la Commission invite à tirer en droit les conséquences de la modification de la nature des données et des informations qui se rapportent aux individus à l'ère numérique (***a***) en retenant une conception large du champ des informations personnelles protégées par notre droit (***b***) afin d'y maintenir l'ensemble des données, traces, éléments ou informations personnels, qu'ils soient identifiants ou suffisent à singulariser ou à différencier les individus sur les réseaux (***c***). Elle recommande également de renforcer l'efficacité des techniques d'anonymisation, condition *sine qua non* du régime dérogatoire applicable aux données personnelles anonymisées (***d***).

a. La modification de la nature des données personnelles traitées à l'ère numérique

Avec les transformations récentes du numérique, la donnée personnelle a changé de visage. Elle ne s'apparente plus seulement à une information ou un élément fourni par l'individu lui-même et collecté dans un fichier et son caractère identifiant n'est plus toujours facile à appréhender.

D'une part, **les individus ne voient pas seulement les informations qu'ils fournissent volontairement faire l'objet de collectes et de traitements par des tiers ; ils laissent également de nombreuses autres traces** de toutes sortes, en navigant sur internet (*IP tracking*, *cookies*), en accédant à des contenus ou en recourant à certains services de géolocalisation. C'est ainsi que la Cour de justice de l'Union européenne (CJUE) a considéré l'adresse IP comme une donnée

---

(1) Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional, Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

à caractère personnel [1] dans la mesure où elle permet aux fournisseurs d'accès de retrouver la personne qui l'utilise [2]. Le même constat s'impose pour les données utilisées à des fins de publicité comportementale et personnalisée. Même s'ils ne permettent pas de connaître directement l'identité civile d'un internaute, les *cookies* sont directement attachés à un matériel et donc à une (ou des) personne(s). Le stockage d'informations (comme les *cookies*) sur l'équipement d'un utilisateur ou l'accès à des informations déjà stockées n'est d'ailleurs possible qu'après le consentement de l'utilisateur [3], depuis la transposition en droit français du « paquet télécom » par l'ordonnance n° 2011-1012 du 24 août 2011 [4]. Pareillement, les pseudonymes (*login*, code, etc.), servant à l'identification de l'utilisateur d'un service, correspondent à des données à caractère personnel qui permettent de le distinguer et de le traiter de manière personnalisée.

D'autre part, **toutes les données ainsi collectées ne présentent pas le même degré d'identification directe des personnes auxquelles elles se rapportent**. Dans certains cas, elles peuvent être directement identifiantes ou le devenir après un traitement particulier. Ainsi, même lorsqu'elles sont censées être anonymisées, certaines données collectées peuvent parfois être rendues de nouveau identifiantes grâce au progrès des techniques de désanonymisation ou parce que d'autres données auxiliaires sont devenues disponibles (par exemple dans le cadre de l'*open data*). Il paraît d'ailleurs difficile de justifier techniquement qu'un jeu de données est absolument anonyme dès lors qu'il est issu de données personnelles : il a par exemple été démontré qu'un petit nombre de métadonnées – en l'espèce quatre positions géographiques – suffisaient à identifier de manière unique, dans 95 % des cas, l'identité d'un individu utilisant un réseau de téléphonie mobile [5] ou encore que 97 % des citoyens d'une ville américaine pouvaient être identifiés de manière unique à partir de seulement deux informations [6].

---

(1) CJUE, 29 janvier 2008, Promusicae c. Telefónica, *n° C-275/06 et CJUE, 24 novembre 2011,* Scarlet c. SABAM, *n° C-70/10.*

(2) Elle n'est par exemple pas considérée comme une donnée à caractère personnel par la cour d'appel de Paris (CA Paris, 27 avril et 15 mai 2007).

(3) Sauf si ces actions visent à permettre ou à faciliter la communication par voie électronique ou sont strictement nécessaires à la fourniture d'un service demandé expressément par l'utilisateur.

(4) Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

(5) Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen et Vincent D. Blondel, « Unique in the crowd : the privacy bounds of human mobility », Nature, *25 mai 2013.*

(6) Il s'agissait en l'espèce des électeurs de la ville de Cambridge dans le Massachusetts, dont 97 % avaient pu être identifiés par le seul croisement de leur date de naissance et des neuf chiffres du code postal de leur adresse : Latanya Sweeney, « Weaving technology and policy together to maintain confidentiality », Journal of Law, *Medicine and Ethics, 25, 1997, pp. 98–110, cité par Kieron O'Hara,* Transparent Government, not Transparent Citizens : A Report on Privacy and Transparency for the Cabinet Office, *2011*.

Par ailleurs, **les données personnelles, imbriquées les unes aux autres, ne renseignent plus seulement sur un individu mais sur un réseau de personnes liées à celui-ci** : comme il a été affirmé au cours de la table ronde sur les « données personnelles et les activités économiques » organisée par la Commission le 18 décembre 2014, les données personnelles ne peuvent plus être « *considérées comme des entités autonomes à la manière des fiches individuelles cartonnées des fichiers du XXe siècle* » (1) ; « *d'un découpage de l'information en données, nous sommes passés à un traitement de l'information à partir de gisements de données* » (2). De plus, l'affaiblissement de la protection de la vie privée d'une personne peut avoir une incidence sur celle des autres. Par exemple, l'acceptation par certains d'une forme de surveillance en échange d'un bénéfice peut devenir un comportement de plus en plus fréquent, voire une norme qui s'imposera finalement à tous. Il convient donc de se garder d'une vision trop individualiste de la protection de la vie privée.

b. La protection actuelle des données identifiantes

Notre législation s'est en partie adaptée, il y a une dizaine d'années, à cette reconfiguration des données personnelles en étendant le champ des données soumises à protection. Lors de la transposition en droit interne de la directive 95/46/CE du 24 octobre 1995 précitée, le législateur a modifié en 2004 (3) le champ des informations protégées par la loi dite « Informatique et libertés » en substituant à la notion d'« *informations nominatives* » celle, plus large, de « *données à caractère personnel* » afin de tenir compte du développement des mesures d'identification indirecte. Aux termes de l'article 2 de ladite loi, les données à caractère personnel correspondent à « *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* ». De manière plus restrictive, l'article 2 de la directive 95/46/CE du 24 octobre 1995 précitée dispose qu'une donnée à caractère personnel est « *toute information concernant une personne physique identifiée ou identifiable (…) qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ».

Dans le cadre de la révision de cette directive, l'article 4 de la proposition de règlement général sur la protection des données (4), dans sa version adoptée par le Parlement européen le 12 mars 2014, propose d'adapter cette définition en prévoyant que constitue une donnée à caractère personnel « *toute information se*

---

(1) Intervention de M. Pierre Bellanger, président-directeur général du groupe Skyrock.

(2) Intervention de M. Paul-Olivier Gibert, directeur de Digital & Ethics.

(3) Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(4) Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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)0011 – C7-0025/2012 – 2012/0011(COD)).

rapportant à une personne physique identifiée ou identifiable (…) qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, par exemple à un nom, à un numéro d'identification, à des données de localisation, à un identifiant unique ou à un ou plusieurs éléments spécifiques, propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle, sociale ou de genre de cette personne ».

c. Retenir une interprétation large de la notion de donnée à caractère personnel

Dans le même esprit que celui de la proposition de règlement général sur la protection des données, la Commission recommande qu'**une interprétation suffisamment large de la notion de donnée à caractère personnel soit retenue pour y inclure l'ensemble des données, traces, éléments ou informations se rapportant directement ou indirectement à un individu, qu'ils soient identifiants ou permettent simplement de le singulariser ou de lui appliquer un traitement différencié**.

Un traitement identique devrait être réservé aux données permettant d'identifier les personnes et à celles permettant simplement de les singulariser ou de leur appliquer des traitements différenciés. Alors que l'Union européenne a envisagé un traitement distinct pour les données à caractère personnel et les données pseudonymes, la Commission souhaite au contraire que ces deux catégories de données soient soumises aux mêmes obligations. Comme la CNIL, elle met en garde contre les risques liés à la création d'une sous-catégorie de données à caractère personnel alors même que les données pseudonymes permettent parfois d'obtenir ou d'extraire des informations précises sur les personnes, voire des informations sensibles comme les données de santé, et donc de les discriminer. Une telle distinction risquerait en outre de conduire, à terme, à un allégement non justifié des obligations à la charge du responsable de traitement et sous-estimerait les capacités croissantes de croisement des données et de réidentification des personnes concernées [(1)]. Enfin, elle introduirait une confusion entre ces données pseudonymes (choisies par l'internaute), et les données pseudonymisées (les identifiants transformés en codes par un processus spécifique et rigoureux de minimisation afin de protéger l'internaute, même s'il résulte toujours d'un compromis entre cette protection contre l'identification et l'utilité des données [(2)]).

Recommandation n° 48

Retenir une interprétation large de la notion de donnée à caractère personnel afin d'y inclure l'ensemble des données, traces, éléments ou informations personnels directement ou indirectement identifiants ou qui permettent de singulariser ou de discriminer un individu parmi d'autres, y compris les données pseudonymes.

---

(1) Latanya Sweeney, « Computational disclosure control : a primer on data privacy protection » (2001) et Paul Ohm, « Broken promises of privacy: responding to the surprising failure of anonymization » (2010).

(2) CNIL, Rapport d'activité 2013, *« La proposition de règlement européen », pp. 26-31.*

d. Renforcer l'efficacité des techniques d'anonymisation des données personnelles

Si les principes relatifs à la protection des données à caractère personnel n'ont pas vocation à s'appliquer lorsque ces données ont été rendues anonymes, encore faut-il que **le processus d'anonymisation présente des garanties sérieuses** afin de limiter les risques de réidentification.

La Commission est consciente des difficultés techniques et des fragilités liées aux principales techniques d'anonymisation utilisées à l'heure actuelle, consistant principalement dans l'occultation de certains champs de données directement identifiantes, l'utilisation de pseudonymes ou la généralisation des données afin qu'elles ne soient plus spécifiques à une personne mais communes à un nombre suffisant d'individus. Elle renouvelle les recommandations qu'elle a précédemment formulées sur la conciliation de la protection de la vie privée et de l'ouverture des données publiques (voir la recommandation n° 4) [(1)]. Ainsi, face aux risques de réidentification, elle recommande de **promouvoir le recours à des techniques sécurisées et fiables**. À cette fin, elle propose que toute technique d'anonymisation soit intégrée dans un processus d'analyse de risques qui permette de s'assurer que les techniques utilisées sont proportionnées aux risques (probabilité d'occurrence et gravité pour les personnes) de désanonymisation. À cet égard, il convient notamment de prendre en compte les **critères** dégagés par le G29 [(2)] : **l'individualisation**, qui concerne la possibilité d'isoler un individu, **la corrélation** ou possibilité de relier entre elles des informations concernant un même individu, **et l'inférence**, c'est-à-dire la déduction de nouvelles informations sur un individu. Les autorités de contrôle devraient accompagner les responsables de traitements dans la mise en œuvre de ces techniques, valoriser les méthodes d'analyse de risques et les processus d'anonymisation les plus efficaces, par exemple sous la forme de labels, et vérifier qu'une veille régulière des données est réalisée afin de garantir dans le temps leur caractère anonyme.

Recommandation n° 49

Afin de réduire les risques de réidentification, promouvoir le recours à des techniques d'anonymisation robustes dans le contexte d'analyses de risques rigoureuses et valoriser les meilleures méthodes, par exemple sous la forme de labels. Les techniques d'anonymisation disponibles actuellement étant insuffisantes, renforcer l'effort de recherche dans ce domaine.

---

(1) Voir supra, *le* b *du 3 du A du I.*

(2) Voir l'avis du G29 du 16 avril 2014 sur les techniques d'anonymisation.

3. Recourir à de nouveaux instruments de protection de la vie privée et des données

Les évolutions récentes du numérique – singulièrement la masse des données collectées et la puissance des responsables de traitements de données publics et privés – conduisent à s'interroger sur l'efficacité des instruments de protection des données personnelles, au regard des technologies aujourd'hui utilisées par ces acteurs pour collecter et traiter les données disponibles, des moyens alloués aux autorités de protection pour réguler ce secteur et du caractère national de cette protection. En réponse à ces trois problématiques, la Commission propose d'encourager plus fortement l'utilisation de technologies renforçant la capacité des personnes à limiter et contrôler l'utilisation de leurs données par des tiers (***a***), de faire évoluer la régulation des responsables de traitements (***b***) et de mettre en place une protection harmonisée des citoyens au niveau européen (***c***).

a. Encourager le recours aux technologies protectrices de la vie privée et des données personnelles

Les technologies numériques ne sont pas seulement propices au développement d'usages ou de traitements dangereux pour la vie privée. Elles permettent également à leurs utilisateurs de mieux maîtriser la manière dont ils s'exposent sur les réseaux ou les conditions dans lesquelles leurs données personnelles peuvent être collectées, traitées et conservées par des acteurs publics ou privés. À cette fin, une variété de techniques a été développée [(1)] : il serait souhaitable de les utiliser dans une démarche intégrant l'exigence de protection de la vie privée dès la conception de l'application ou du logiciel (*privacy by design* [(2)]) ou dans ses paramètres par défaut (*privacy by default*).

Les techniques de protection de la vie privée permettent soit de limiter la collecte de données personnelles, selon le principe de « minimisation des données », soit de renforcer la maîtrise de l'individu sur ses données [(3)]. Parmi les solutions de minimisation, figurent notamment les outils de chiffrement des communications [(4)], de calcul sécurisé multi-parties [(5)] ou de chiffrement

---

(1) George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner, « Privacy and data protection by design – from policy to engineering », in ENISA Report*, décembre 2014.*

(2) Daniel Le Métayer, « Privacy by design : a matter of choice », in Data protection in a profiled world*, Serge Gutwirth, Yves Poullet, Paul De Hert (eds.), Springer, 2010, pp. 323-334.*

(3) Dans l'objectif d'une privacy by design*, des techniques émergentes visent à « décentraliser » la protection des données (http://web.media.mit.edu/~guyzys/data/ZNP15.pdf) sur la base de la technologie* BlockChain*, sur laquelle se fondent également les crypto-monnaies de type* Bitcoin *et qui ont démontré, sans être vulnérables, leur intérêt au regard de la sécurité des données.*

(4) Ces techniques peuvent être utilisées pour protéger le contenu des informations (confidentialité) ou l'identité des parties impliquées (anonymat).

(5) Le calcul sécurisé multi-parties permet à plusieurs entités d'effectuer un calcul sur leurs données sans que quiconque ne divulgue ses propres données. À titre d'illustration, plusieurs personnes peuvent déterminer de façon collective celle qui possède la plus grande fortune sans qu'aucune d'entre elles ne révèle sa propre fortune aux autres.

homomorphe [1]. Certaines de ces techniques sont déjà utilisées (comme *Tor* pour assurer l'anonymat des communications) ou peuvent l'être (comme le chiffrement homomorphe pour protéger les consommateurs dans les infrastructures de compteurs intelligents) ; d'autres doivent donner lieu à de nouveaux travaux de recherche, notamment pour améliorer leur efficacité et leur ergonomie.

Pour ce qui est des outils de contrôle sur les données personnelles, la première nécessité est de fournir des informations suffisantes aux personnes pour leur permettre d'apprécier la situation et les conséquences d'un choix. Certains outils ou sites comme *Cookieviz* [2], *Lightbeam* [3] ou *Panopticlick* [4] existent déjà et contribuent à améliorer cette transparence. Certains, comme *ToS;DR* [5], promeuvent une démarche collective en permettant aux experts et à toute personne prenant la peine de les analyser de noter les politiques de vie privée des sites, fournissant ainsi à chacun des éléments d'appréciation utiles. D'autres outils permettent aux individus d'exprimer des choix (comme *Do Not Track*), de gérer eux-mêmes leurs *cookies* (refus d'installation, effacement) ou encore de manière plus générale d'héberger leurs données personnelles où ils le souhaitent, de décider librement de leur utilisation et diffusion à des tiers et de choisir avec quelles autres données elles peuvent s'interconnecter. Dans cet esprit d'« *empowerment* » des individus, ou de réduction de l'asymétrie intrinsèque qui existe actuellement entre ces derniers et les responsables de traitement, des initiatives comme « *Mes Infos* » en France (lancée par la FING, Fondation internet nouvelle génération) ou *My Data* au Royaume-Uni, reposent sur le principe selon lequel les entreprises et les administrations qui détiennent des informations sur les personnes doivent les partager avec ces personnes pour leur permettre d'en tirer bénéfice elles-mêmes.

On assiste donc à un foisonnement de propositions d'outils et de techniques de protection de la vie privée. Toutefois, force est de constater que ces technologies peinent à se déployer, pour des raisons à la fois juridiques, liées à l'absence de caractère contraignant des règles posées en la matière, et économiques, tenant à l'insuffisante incitation faite aux industries d'investir dans ce type de technologies, ainsi qu'en raison de difficultés techniques.

Il est donc nécessaire de stimuler le recours à ces technologies et de favoriser le développement du *privacy by design*. L'idée d'inscrire la protection de

---

(1) Le chiffrement homomorphe permet de réaliser des calculs sur des données chiffrées sans déchiffrer celles-ci. Il peut être appliqué par exemple aux infrastructures de compteurs intelligents pour permettre au fournisseur d'énergie de calculer le montant dû par un abonné sans avoir à connaître ses consommations individuelles.

(2) Cookieviz *est un outil développé par la CNIL qui permet de visualiser les* cookies *qui transmettent des informations à des tiers.*

(3) Lightbeam *permet de visualiser de manière interactive les sites tiers avec lesquels un internaute communique (généralement à son insu).*

(4) Panopticlick *montre à un internaute à quel point la configuration de son navigateur est unique et permet de le tracer (sans avoir recours à des* cookies*).*

(5) Terms of Service ; Didn't Read.

la vie privée dans les systèmes d'information n'est pas nouvelle [1]. Elle figurait déjà à l'article 17 de la directive 95/46/CE du 24 octobre 1995 précitée qui dispose que « *le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite* ».

La Commission propose d'**encourager la conception et l'utilisation de technologies donnant à tout internaute une réelle maîtrise sur l'utilisation de ses données ainsi que leur certification par des tiers indépendants, condition nécessaire à l'instauration d'une confiance et d'un différenciateur commercial pour ces technologies**. Diverses mesures incitatives ou obligatoires pourraient ainsi élargir le recours à ce type de technologies. À titre d'exemple, le législateur européen envisage, à l'article 23 de la proposition de règlement général sur la protection des données, dans sa rédaction adoptée par le Parlement européen le 12 mars 2014, d'en promouvoir la conception et l'utilisation, en formulant plusieurs exigences en la matière et en faisant de la protection des données dès la conception une condition préalable aux offres de marchés publics. Ces mesures devraient s'appliquer non seulement aux responsables de traitements mais également aux fournisseurs de technologies.

Recommandation n° 50

Encourager la conception et l'utilisation de technologies permettant de rendre effectif le principe de minimisation de la collecte de données personnelles et donnant à tout individu une réelle maîtrise sur l'utilisation de ses données (*privacy by design* et *privacy by default*) par la mise en place de dispositifs plus contraignants ou réellement incitatifs à destination des responsables de traitements et des fournisseurs de technologies et par l'instauration d'un schéma de certification de ces technologies accessible pour de petites entreprises et des projets de développements communautaires de logiciels libres.

Par ailleurs, les technologies de chiffrement des données, qui constituent des solutions intéressantes dans la protection à la source des informations personnelles qui transitent par les réseaux, devraient être davantage utilisées. La Commission n'ignore pas que ces procédés, dont l'utilisation permet en particulier de rendre anonymes les échanges sur internet, peuvent être employés à des fins contraires à l'ordre public, rendant plus compliquée l'action de l'autorité judiciaire dans la lutte contre certaines activités illégales. Elle rappelle toutefois qu'il s'agit de technologies légales, protégées et encadrées par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dont l'article 30

(1) Voir à ce sujet, en annexe, la contribution écrite de Mme Francesca Musiani au groupe de travail sur la vie privée.

dispose que « *l'utilisation des moyens de cryptologie est libre* ». Sous réserve de satisfaire aux conditions posées par cette loi et de ne pas empêcher toute action de l'autorité judiciaire dans la lutte légitime contre certains contenus illégaux, la Commission recommande d'**inciter le recours aux technologies de chiffrement afin de renforcer la confidentialité des communications** entre individus face aux nombreux procédés susceptibles de la remettre en cause. Plusieurs conditions cumulatives devraient être réunies :

– la définition impartiale et indépendante de normes, critères, protocoles et niveaux de chiffrement des données de nature à prévenir toute corruption des données ;

– la possibilité de chiffrement « de bout en bout » de l'ensemble des communications privées ;

– l'enseignement du chiffrement à l'école, pour s'assurer que cette pratique est réellement utilisée par les individus ;

– le contrôle par l'usager de ses clés de chiffrement.

Recommandation n° 51

Dans le respect des compétences de l'autorité judiciaire en matière de lutte contre les activités et contenus illégaux, inciter au recours à des technologies de chiffrement des données afin de renforcer la confidentialité des communications.

Enfin, la Commission suggère de mieux encadrer les modalités techniques d'organisation des réseaux numériques, la conception générale des systèmes d'information et la définition de leur architecture afin de renforcer la sécurité de leur fonctionnement face aux attaques malveillantes dont ils peuvent faire l'objet et ainsi préserver la sécurité et la confidentialité des données personnelles qui transitent par eux. Ces dernières années, un nombre trop important d'entreprises ou d'opérateurs publics ont vu les données personnelles qu'ils avaient collectées auprès de leurs clients ou usagers piratées.

Une proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union [(1)] est en cours de discussion au niveau de l'Union européenne afin d'établir un niveau de compétences et des capacités minimales de réaction dans chaque État, de mettre en place une coordination au niveau européen obligatoire – aujourd'hui, seuls neuf États se concertent – et de poser une obligation générale de gestion des risques et de notification des infractions graves à la législation.

---

(1) Résolution législative du Parlement européen du 13 mars 2014 sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)).

Au-delà de la nécessaire coordination de l'action des États membres en matière de cybersécurité, la Commission suggère plus particulièrement de **renforcer les obligations de sécurité à la charge des acteurs de l'internet assumant des fonctions d'intermédiation** (*internet enablers*), comme les moteurs de recherche, les magasins en ligne ou les réseaux sociaux.

En outre, en complément du renforcement des obligations de sécurité et de confidentialité des données, l'ensemble des responsables de traitements – et pas seulement les fournisseurs d'accès à internet et de téléphonie fixe ou mobile [(1)] – devrait être soumis à une obligation de notification aux autorités de régulation compétentes de tout accès non autorisé aux données personnelles, toute perte ou altération, qu'ils procèdent d'un acte malveillant ou d'une erreur matérielle. Cette notification devrait également être adressée aux personnes dont les données ont été violées, lorsque la violation peut avoir une incidence sur les personnes. La Commission salue à cet égard les pistes d'évolution formulées dans ce domaine par les articles 31 et 32 de la proposition de règlement général sur la protection des données dans sa version adoptée par le Parlement européen le 12 mars 2014.

Recommandation n° 52

Mettre les architectures et les modèles d'organisation des réseaux numériques au service de la protection de la vie privée ; renforcer les obligations de sécurité à la charge des acteurs de l'internet assumant des fonctions d'intermédiation ; généraliser l'obligation de notification des failles de sécurité.

b. Repenser la régulation des responsables de traitements

La Commission s'est également intéressée au mode de régulation des activités des responsables de traitements. Si elle estime indispensable de maintenir cette régulation et de continuer à la confier à une autorité de protection spécialisée, elle propose d'en repenser les contours afin de l'adapter aux nouvelles exigences du secteur.

Aujourd'hui, la CNIL occupe une large part de son activité de conseil et de réglementation aux procédures de formalités préalables instaurées par les articles 22 à 31 de la loi dite « Informatique et libertés ». Depuis 2004 en effet, tous les fichiers – publics comme privés – sont soumis à un régime de déclaration préalable [(2)] dont sont cependant dispensés les responsables de traitements qui ont

---

(1) Depuis la transposition du « paquet télécom » de 2009 par l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, l'article 34 bis *de la loi n° 78-17 du 6 janvier 1978 précitée impose aux fournisseurs d'accès à internet et de téléphonie fixe ou mobile de notifier aux autorités de régulation compétentes les violations de données personnelles intervenues dans le cadre de leur activité de services de communications électroniques, c'est-à-dire toute destruction, perte, altération ou accès non autorisé à des données à caractère personnel, qu'ils procèdent d'un acte malveillant ou d'une erreur matérielle.*

(2) Originellement, la loi n° 78-17 du 6 janvier 1978 précitée soumettait les traitements du secteur public à un régime d'autorisation préalable et ceux du secteur privé à un régime de déclaration.

désigné un correspondant à la protection des données à caractère personnel. Certains fichiers particulièrement sensibles doivent cependant être autorisés par la CNIL, par un arrêté ministériel ou par décret en Conseil d'État pris après avis de la CNIL (données sensibles mentionnées par l'article 8, données biométriques, utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques, interconnexion de fichiers, etc.) [(1)].

Cette logique de déclaration préalable est contestée, au motif qu'elle conduirait à transmettre au régulateur un nombre considérable d'informations d'inégal intérêt, ne lui permettant pas toujours d'évaluer la sensibilité du traitement à défaut de connaître par exemple le nombre de personnes dont les données sont susceptibles d'être traitées ou le volume des données transmises à des tiers. Il ferait également peser sur les acteurs concernés une obligation relativement lourde, proportionnelle à l'ampleur de l'activité conduite dans le secteur numérique.

La CNIL a adapté ce régime en établissant des normes simplifiées de déclaration « *pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés* » et des dispenses de déclaration pour certains traitements sans danger pour la vie privée ou en permettant de procéder à une déclaration unique des traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles [(2)]. À partir de 2011, elle a également développé ses missions de conseil, d'accompagnement et de suivi, afin que la protection des données personnelles passe non seulement par le respect de formalités administratives préalables mais aussi par une relation en continu entre le secteur concerné et le régulateur : développement de *packs* de conformité, aide à l'édiction de codes de conduite définissant la politique d'une entreprise en la matière, sous la forme de règles contraignantes d'entreprises (RCE) ou *binding corporate rules* (BCR [(3)]), de codes de déontologie ou de chartes, délivrance de labels à des procédures d'audit et de formations [(4)], etc.

Ces instruments, même s'ils procèdent d'une démarche pragmatique, sont parfois contestés car ils reposent sur des déclarations d'intentions des responsables de traitements, déclarations qui permettent à ceux-ci d'améliorer leur image auprès du public ou de transférer plus facilement des données personnelles sans pour autant apporter de véritables garanties aux individus. Pour les rendre effectifs, ils devraient être complétés par une **responsabilisation** (***accountability***) des exploitants de traitements.

---

(1) Articles 25 à 27 de la loi n° 78-17 du 6 janvier 1978 précitée.

(2) Articles 23 et 24 de la loi n° 78-17 du 6 janvier 1978 précitée.

(3) Les règles contraignantes d'entreprises sont des programmes de conformité permettant de décliner les principes de protection des données personnelles sous forme de règles internes à un groupe d'entreprises.

(4) CNIL, Rapport d'activité 2011, *« Au-delà de la loi : la protection des données et de la vie privée, valeur de l'entreprise », pp. 90-92 ; CNIL,* Rapport d'activité 2012, *« 2012 : l'année des premiers labels », pp. 36-37.*

La responsabilisation (*accountability*) [1] est une notion qui désigne « *l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données* » [2]. En vertu de cette logique, le responsable de traitements de données à caractère personnel devrait, en amont, prendre des mesures proactives de protection des données qu'il collecte – notamment par la désignation d'un délégué à la protection des données si elle ne lui a pas déjà été imposée, la réalisation d'études d'impact ou d'audits réguliers de ses traitements – et, en aval, rendre des comptes sur ses pratiques. Pour la Commission, il s'agit de formes intéressantes et importantes de protection de la vie privée « par la preuve », permettant aux entreprises de démontrer qu'elles respectent la réglementation applicable à la collecte et au traitement de données à caractère personnel et ainsi de susciter la confiance des consommateurs, à condition toutefois que soient prévues des mesures de contrôle (audits) par des tiers indépendants, dans l'esprit de la certification des comptes financiers par les commissaires aux comptes des entreprises.

Dès lors, si la Commission est favorable à la simplification des procédures de déclaration préalable en passant **d'une logique formelle de déclaration à une logique de mise en conformité et de respect en continu de la réglementation, c'est à condition de compenser cette évolution par une véritable responsabilisation des exploitants de traitements de données personnelles pour assurer qu'elle ne se traduit pas par un affaiblissement des droits des personnes**.

À cette fin, plusieurs mesures concrètes pourraient être prises, comme rendre obligatoire la désignation d'un délégué à la protection des données [3] pour les responsables de traitements d'une certaine taille et ceux qui, n'atteignant pas cette taille, mettraient en œuvre un traitement concernant un nombre important d'individus ou présentant un certain degré de sensibilité, ou généraliser les procédures de certification par lesquelles un tiers accrédité par l'autorité de protection atteste que le responsable du traitement s'est conformé à la réglementation. Une démarche responsable des exploitants des traitements devrait comporter une analyse d'impact préalable et une analyse de risques détaillée des traitements mis en place, accompagnées de justifications précises des choix effectués au regard de ces risques et des contremesures adoptées pour les minimiser.

---

(1) Voir à ce sujet, en annexe, la contribution écrite de M. Cyril Zimmermann au groupe de travail sur la vie privée ainsi que Denis Butin, Marcos Chicote, Daniel Le Métayer, « Strong accountability : beyond vague promises », in Reloading data protection, *Serge Gutwirth, Ronald Leenes, Paul De Hert (eds.), Springer, 2014, pp. 343-369.*

(2) CNIL, Rapport d'activité 2014, *p. 89.*

(3) Désigné en France sous le nom de correspondant informatique et libertés.

Recommandation n° 53

Passer d'une logique formelle de déclaration à une logique de mise en conformité et de respect en continu de la réglementation.

En contrepartie, accroître la responsabilisation des exploitants de traitements de données personnelles par la généralisation des obligations de rendre compte des traitements effectués sur les données personnelles ou qui peuvent avoir une incidence sur la vie privée des individus (*accountability*) et la mise en place de procédures d'audits par des tiers indépendants ; prévoir une sensibilisation à ces questions, notamment par un renforcement de la formation continue délivrée sur ce sujet.

En revanche, **les traitements les plus sensibles et ceux présentant des risques élevés pour la protection de la vie privée et des données à caractère personnel devraient quant à eux demeurer soumis à des obligations renforcées**. La Commission, particulièrement attachée à la logique de protection uniforme des individus face aux activités numériques, n'est en effet pas opposée par principe à l'introduction dans notre législation d'une analyse des risques auxquels ceux-ci sont exposés : diffusion de données contre leur gré ou en dehors de leur volonté, utilisation abusive ou malveillante de données, risques de réputation, de discrimination pour l'accès à certains services (crédits, assurances, emploi), pratiques commerciales abusives de différenciation entre clients, etc. [(1)]. Elle doit cependant être mise au service d'une plus grande protection de la vie privée et non d'un affaiblissement de celle-ci. C'est la raison pour laquelle la Commission pose **deux limites à l'encadrement des traitements de données en fonction des risques qu'ils présentent** :

– **il ne saurait conditionner l'exercice des droits reconnus à chaque individu à l'existence avérée d'un risque**, dans la mesure où, comme l'a justement relevé devant la Commission Mme Isabelle Falque-Pierrotin, « *une protection limitée aux cas présentant un risque diffère du tout au tout avec le système actuel où l'individu a des droits indépendamment du risque encouru ou du mal subi du fait d'un traitement* » ;

– **il ne devrait pas avoir pour effet d'exonérer le responsable du traitement de l'ensemble de ses obligations de mise en conformité à la législation** relative à la protection des données.

Recommandation n° 54

Soumettre à des obligations particulières les responsables de traitements de données personnelles exposant l'individu à des risques ou à des préjudices particuliers. À cet effet, rendre obligatoire l'analyse de risques préalable permettant d'identifier ces risques et préjudices.

---

(1) Voir à ce sujet, en annexe, la contribution écrite de M. Daniel Le Métayer au groupe de travail sur la vie privée.

La Commission salue à cet égard les pistes retenues par la proposition de règlement général sur la protection des données dans sa rédaction adoptée par le Parlement européen le 12 mars 2014, qui envisage de créer un nouveau principe de responsabilité exigeant que les données soient « *traitées sous la responsabilité du responsable du traitement, qui veille à la conformité avec les dispositions du présent règlement et est en mesure d'en apporter la preuve* » (1). Elle prévoit également de supprimer l'obligation de déclaration préalable des traitements à l'autorité de contrôle pour la remplacer par une obligation de consultation de celle-ci pour les seuls traitements présentant des risques particuliers. Elle propose de renforcer la responsabilisation des organismes, tenus de mettre en œuvre des mécanismes et procédures internes garantissant le respect des règles relatives à la protection des données à caractère personnel. Elle rend également obligatoire la désignation d'un délégué à la protection des données pour tous les organismes publics et les traitements des entreprises privées touchant plus de 5 000 personnes sur une période de douze mois consécutifs, ou dont les activités de base consistent en des traitements impliquant un suivi régulier et systématique des personnes.

Les sanctions susceptibles d'être prononcées en cas de non-respect de la législation relative à la protection des données à caractère personnel paraissent elles aussi relativement inadaptées à la potentielle gravité des violations de la législation et à la puissance de certains responsables de traitements qui s'en rendent coupables.

Certes rares sont les procédures de contrôle lancées par le régulateur à l'encontre d'un traitement de données personnelles qui aboutissent au prononcé de sanctions. En effet, la procédure de contrôle est fortement marquée par une logique de mise en conformité du responsable de traitements et de dialogue entre celui-ci et le régulateur.

Si de nombreux contrôles sont réalisés par la CNIL, dont près d'un tiers à la suite d'une plainte, la plupart des situations sont résolues par des échanges entre l'organisme concerné et la CNIL, sous la forme d'échanges de courriers invitant celui-ci à se mettre en conformité avec la loi. À défaut, la CNIL procède à des contrôles dans ses locaux, à la suite desquels, en cas de manquement mineur, elle envoie un courrier d'observations demandant à l'organisme de se mettre en conformité ; à défaut de réponse satisfaisante de ce dernier, il peut alors être procédé à une mise en demeure à laquelle l'organisme devra obéir dans un délai déterminé. En l'absence de mise en conformité, une procédure de sanction est engagée devant la formation restreinte de la CNIL – la mise en demeure n'étant toutefois pas un préalable nécessaire à l'engagement d'une procédure de sanction.

En pratique, la CNIL observe un taux important de mise en conformité aux remarques formulées par ses services à l'occasion d'un contrôle, ce qui montre l'utilité de l'accompagnement et de la phase précontentieuse (voir l'encadré ci-après).

---

(1) Article 5 de la proposition de règlement général sur la protection des données.

Les missions de contrôle et de sanction de la CNIL en 2013 et 2014

En 2013 (1)

La CNIL a reçu **5 640 plaintes** : la première intervention de la CNIL a suffi dans 99 % des cas à résoudre le problème. Sur les 414 contrôles qui ont été réalisés (dont 33 % à la suite de plaintes), 89 % ont débouché sur une mise en conformité rapide ; seules 57 mises en demeure ont été prononcées – dont 8 ont été rendues publiques – ayant entraîné la mise en conformité des organismes concernés dans 86 % des cas. **14 dossiers** ont fait l'objet d'une procédure de **sanction**.

En 2014 (2)

La CNIL a reçu **5 825 plaintes** ; elle a procédé à 421 contrôles, dont 28 % dans le cadre du programme annuel de contrôle, 24 % à la suite de plaintes, 40 % à l'initiative de la CNIL au vu de l'actualité notamment, 6 % à la suite d'un courrier d'observations adressé après un premier contrôle et 2 % dans le cadre des suites de mises en demeure ou de procédures de sanction. 62 mises en demeure ont été prononcées, dont 68 % ont débouché sur une mise en conformité rapide du responsable de traitement. En définitive, **18 dossiers** ont fait l'objet d'une procédure de **sanction**, à raison de 8 sanctions pécuniaires, 7 avertissements et 3 relaxes.

(1) CNIL, Rapport d'activité 2013*, « Contrôler et sanctionner », pp. 50-55.*

(2) CNIL, Rapport d'activité 2014*, « Contrôler et sanctionner », pp. 51-54.*

Cependant, il arrive que le responsable du traitement refuse de se mettre en conformité avec les exigences posées par la CNIL ou ait violé manifestement et gravement les règles relatives à la protection des données à caractère personnel. Dans cette hypothèse, le régulateur peut décider de sanctionner le responsable du traitement incriminé. Mais en l'état actuel du droit, les pouvoirs de sanction pécuniaire de la CNIL, limités à 150 000 euros ou 300 000 euros en cas de réitération (1), sont insuffisamment dissuasifs pour certains puissants acteurs du numérique pour lesquels ces plafonds correspondent à une part négligeable des bénéfices dégagés chaque année.

En conséquence, la Commission **souhaite que le législateur révise au plus vite le montant des sanctions pécuniaires susceptibles d'être prononcées à l'égard d'un responsable de traitement qui ne respecte pas la loi**. Elle estime que la proposition de règlement général sur la protection des données, dans sa version adoptée par le Parlement européen le 12 mars 2014, constitue une avancée significative en prévoyant d'en porter le plafond à 100 millions d'euros ou à 5 % du chiffre d'affaires annuel mondial de l'entreprise concernée (2).

Par ailleurs, force est de constater que les sanctions pécuniaires ne sont pas les plus dissuasives pour tous les responsables de traitements et que l'effet négatif d'une publication de décision ou de condamnation peut être plus significatif, notamment en termes d'image. La Commission recommande donc que la publication des constats d'infractions soit plus souvent utilisée en complément des sanctions prononcées.

---

(1) Article 47 de la loi n° 78-17 du 6 janvier 1978 précitée.

(2) Article 79 de la proposition de règlement général sur la protection des données.

Recommandation n° 55

Revoir la nature des sanctions applicables aux responsables de traitements contrevenant à la réglementation :

– augmenter significativement le montant des sanctions pécuniaires que l'autorité de protection peut prononcer à leur encontre ;

– encourager la décision de publication des sanctions consécutives aux constats d'infractions établis à leur encontre.

c. Mettre en place une protection harmonisée des citoyens au niveau européen

Enfin, la Commission a été frappée par la profonde inadéquation entre le caractère national du champ d'application territorial actuel de la protection des données personnelles et le caractère transnational des traitements de données, aussi bien au niveau des normes qu'au niveau du mode d'intervention des autorités de protection. Cette situation est insatisfaisante tant pour l'exercice des droits des individus que pour le développement des entreprises.

S'agissant des normes, la Commission constate avec satisfaction que l'Union européenne va se doter d'un cadre juridique parfaitement harmonisé en remplaçant la directive 95/46/CE du 24 octobre 1995 précitée, qui avait conduit à une transposition inégale de ses dispositions dans chaque État membre, par un règlement d'application immédiate. Elle observe également que la Cour de justice de l'Union européenne (CJUE), le 6 octobre 2015 (1), a invalidé la décision de la Commission de 2000 sur le régime de la « sphère de sécurité » (*Safe Harbor*) (2) qui régissait le transfert de données personnelles vers les États-Unis, au motif que la Commission n'avait pas constaté que ce pays assurait effectivement un niveau de protection des droits fondamentaux équivalent à celui garanti au sein de l'Union en vertu de la directive de 1995. Cette décision appelle en conséquence une profonde révision des conditions de transfert de telles données vers les États-Unis afin d'assurer aux citoyens de l'Union un niveau de protection satisfaisant face aux activités de responsables de traitements américains.

De surcroît, l'article 3 de la proposition de règlement général sur la protection des données, dans sa rédaction adoptée par le Parlement européen le 12 mars 2014, prévoit un champ d'application du règlement élargi à l'ensemble des responsables de traitements implantés sur le territoire de l'Union et aux responsables de traitements non établis dans l'Union « *lorsque les activités du traitement sont liées (...) à l'offre de biens ou de services à* [d]*es personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes*

---

(1) CJUE, 6 octobre 2015, n° C-362/14.

(2) Décision 2000/520/CE de la Commission du 26 juillet 2010 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiées par le ministère du commerce des États-unis d'Amérique.

concernées (...) ou (...) à l'observation de ces personnes concernées ». Toutefois, la Commission recommande de **renforcer l'effectivité de l'application du futur règlement à l'ensemble de ces traitements de données en déclarant expressément nulle et non avenue toute clause contractuelle d'un responsable de traitements qui prévoirait l'application d'une autre loi que la législation européenne**. Cette précision apparaît d'autant plus nécessaire qu'elle permettrait de conférer à ce règlement le caractère d'une loi de police nécessaire à la sauvegarde des intérêts publics protégés par l'Union, c'est-à-dire son application impérative quelle que soit la loi normalement applicable au contrat.

Recommandation n° 56

Faire du futur règlement général européen sur la protection des données une loi de police permettant l'application impérative de ses dispositions indépendamment de la loi applicable en vertu d'une clause contractuelle du responsable du traitement.

Il reste toutefois à mieux coordonner l'intervention des autorités de protection de chaque État membre de l'Union, dont l'existence n'est pas remise en cause par le futur cadre juridique communautaire. À cet effet, la proposition initiale de règlement général sur la protection des données envisageait la création d'un guichet unique lorsque le traitement de données à caractère personnel a lieu dans plusieurs États membres et désignait comme autorité exclusivement compétente faisant office de « guichet unique » celle de l'État membre dans lequel le responsable du traitement ou le sous-traitant avait son principal établissement.

La Commission est particulièrement attentive à ce que chaque citoyen puisse faire valoir ses droits auprès d'une autorité de protection facilement identifiable et qui puisse être saisie par des voies de recours aisément accessibles. Or tel n'était pas le cas de ce « guichet unique », susceptible de conduire, comme l'a souligné la CNIL, à un « *éloignement sensible des citoyens des autorités compétentes* ». « *En cas de problème pour un internaute sur un réseau social dont l'établissement principal est implanté dans un autre État membre*, [sa] *plainte* [aurait été] *traitée par l'autorité de ce dernier et non par l'autorité du lieu de sa résidence* » et « *le citoyen souhaitant contester les résultats de l'instruction de sa plainte* [aurait dû] *alors le faire auprès d'un tribunal étranger* ». Elle ajoutait qu'« *il serait paradoxal que la protection en matière de données personnelles soit finalement plus faible qu'en droit de la consommation qui privilégie une compétence basée sur le lieu de résidence du consommateur* » et qu'un tel critère « *encouragerait (...) les pratiques de* forum shopping [(1)] » [(2)].

En conséquence, la Commission recommande de **conserver la compétence de principe de chaque autorité de protection sur son territoire.**

---

(1) Fait pour une entreprise de choisir son implantation dans un pays qui se distingue par les avantages juridiques de sa législation.

(2) CNIL, Rapport d'activité 2011, *« Révision de la directive : réussir l'Europe de la protection des données », pp. 86-89.*

Lorsque le traitement incriminé a lieu dans plusieurs États membres, une coordination de l'intervention des autorités de protection est alors nécessaire. Dans cette hypothèse, la Commission propose de **concevoir un modèle de gouvernance conciliant la désignation d'un interlocuteur unique pour les responsables de traitements qui s'implantent dans plusieurs États membres et les nécessités liées à l'effectivité de la protection des droits des citoyens et de l'exercice des garanties** qui leur sont offertes. Pour elle, ce modèle devrait respecter plusieurs exigences :

– l'**organisation d'une coopération entre les autorités de protection** sur le territoire desquelles sont mis en œuvre des traitements transnationaux, c'est-à-dire entre les autorités du pays de résidence des personnes visées par le traitement et l'autorité du pays de l'établissement principal de l'entreprise ;

– la **désignation**, parmi ces autorités, **d'une autorité chef de file** qui serait l'interlocuteur unique du responsable de traitement concerné, désigné sur la base du critère de l'établissement principal de ce responsable ;

– la **mise en œuvre d'une procédure de codécision** garantissant l'implication et la participation de toutes les autorités de protection concernées dans un processus décisionnel égalitaire, équilibré et respectueux de leur indépendance ;

– la **préservation d'un recours juridictionnel effectif** des personnes visées par le traitement devant un juge de leur pays de résidence contre les décisions prises par l'autorité chef de file.

Le trilogue en cours entre la Commission européenne, le Conseil de l'Union européenne et le Parlement européen s'achemine vers un système analogue fondé sur l'institution d'une autorité chef de file désignée sur la base du critère de l'établissement principal du traitement. Dans ce schéma, l'autorité chef de file prendrait des mesures après consultation des autres autorités de contrôle compétentes, à charge pour le Comité européen de la protection des données d'émettre un avis sur l'identification de l'autorité chef de file en cas de difficultés ou en cas de dissensions importantes lors de l'examen d'un cas particulier.

Recommandation n° 57

Pour les traitements de données implantés dans plusieurs États, coordonner à l'échelle européenne l'intervention des autorités de protection par l'institution d'un « guichet unique » respectueux du principe de proximité du citoyen avec l'autorité de protection des données ou le juge national dont il dépend.

B. DONNER À L'INDIVIDU L'AUTONOMIE INFORMATIONNELLE ET DÉCISIONNELLE NÉCESSAIRE À SON LIBRE ÉPANOUISSEMENT DANS L'UNIVERS NUMÉRIQUE

La Commission estime également nécessaire d'adapter notre législation afin de tenir compte de l'évolution qu'ont subie au cours de ces dernières années les droits au respect de la vie privée et à la protection des données à caractère personnel, qui s'apparentent de plus en plus à une exigence de libre épanouissement de la personnalité et à un désir d'autonomie individuelle. L'individu ne s'attend pas seulement à voir sa vie privée préservée de toute immixtion extérieure ; il revendique également la liberté de choisir et de contrôler les conditions dans lesquelles ses données personnelles peuvent être collectées et utilisées.

Il n'est pas ici question de remettre en cause la philosophie générale de notre législation, fondée sur la protection de la personne et non sur celle de ses données, mais au contraire de la conforter en lui donnant pour objectif de réparer l'asymétrie informationnelle et décisionnelle qui existe actuellement entre les individus et les responsables de traitements (**1**). Pour ce faire, le primat du consentement préalable de l'individu avant le traitement de ses données doit être conservé mais adapté à l'ère numérique (**2**). Pour que ce consentement soit parfaitement éclairé et effectif, l'individu doit également se voir reconnaître de véritables droits d'information et d'action dans la mise en œuvre de ces traitements (**3**).

1. Privilégier le droit à l'autodétermination de l'individu dans l'usage de ses données personnelles

La Commission est profondément attachée à la préservation de la logique personnaliste qui a toujours présidé à notre réglementation en protégeant non pas les données personnelles dont chacun serait propriétaire mais l'individu dont elles émanent (***a***). Cette logique a aujourd'hui besoin d'être complétée afin qu'elle ne permette pas seulement une protection des personnes mais aussi leur autonomisation dans l'univers numérique (***b***).

a. Écarter la contractualisation du droit au respect de la vie privée

La monétisation économique croissante dont font aujourd'hui l'objet les données personnelles a pu conduire certains à considérer que la protection de la vie privée à l'ère numérique serait mieux assurée par la reconnaissance d'un droit de propriété de l'individu sur ses données permettant de mieux concilier l'exigence de protection avec le souhait de nombreuses personnes de valoriser leurs informations personnelles, en échange d'une rémunération ou d'un service.

À l'unisson des positions déjà exprimées sur cette question par plusieurs organismes, en particulier le Conseil d'État [(1)] et la CNIL [(2)], la Commission

---

(1) Conseil d'État, op. cit., *pp. 264-267.*

(2) CNIL, Rapport d'activité 2013, *« Le choc de l'affaire Prism : vers une surveillance massive et généralisée de l'ensemble de la population », p. 6.*

estime **inopportun et dangereux d'introduire une logique patrimoniale dans la protection des données personnelles**.

Comme l'a indiqué Mme Isabelle Falque-Pierrotin lors de son audition par la Commission le 26 novembre 2014, une telle logique ferait perdre « *des leviers d'action considérables sur lesdites données : étant propriétaire de ses données, l'individu pourrait les vendre, notamment à des acteurs étrangers. Or la grande supériorité intellectuelle du droit à la protection des données personnelles réside dans le fait qu'il reconnaît le droit d'un individu même si les données sont traitées par d'autres* ». Certes la reconnaissance d'un droit de propriété de l'individu sur ses données ne conduirait pas à une privatisation irréversible de ses informations personnelles et à la perte de tout contrôle sur leur devenir. Le droit de la propriété intellectuelle enseigne, dans d'autres domaines, qu'il est possible de ménager des outils d'inaliénabilité limitant la portée du droit de cession, ouvrant des possibilités de licence et, en définitive, modulant cette patrimonialisation.

Mais, ainsi que l'a souligné Mme Maryvonne de Saint-Pulgent, présidente de la section du rapport et des études du Conseil d'État, entendue le 16 octobre 2014, il est incontestable qu'elle fragiliserait considérablement le cadre juridique qui régit aujourd'hui les conditions d'utilisation des données personnelles. Elle se heurterait aux limites territoriales de la reconnaissance du droit de propriété, à l'heure où les grands responsables de traitements de données sont implantés à l'étranger. Et « *la reconnaissance de ce droit de propriété rendrait plus difficile l'action de l'État pour protéger les individus confrontés à de multiples pièges car toutes ses interventions pourraient alors être regardées comme portant atteinte à un droit de valeur constitutionnelle* ».

Par ailleurs, la Commission considère que les principes actuels de la loi dite « Informatique et libertés » permettent déjà une valorisation économique des données, en autorisant, sous certaines conditions, leur recueil, leur exploitation et leur conservation en échange de la délivrance de services ou de facilités. Elle observe du reste qu'un droit de propriété individuel sur les données ne permettrait pas de rééquilibrer la relation asymétrique qui existe aujourd'hui entre les éditeurs de services numériques et les internautes, marquée par la très faible valeur accordée aux données d'un seul individu. Il serait donc pour le moins paradoxal d'accorder un droit de propriété à des individus pris isolément alors que c'est la masse des données de plusieurs centaines d'individus qui constitue une valeur économique aux yeux des responsables de traitements.

Enfin, elle romprait avec l'approche généraliste et personnaliste de notre législation, qui considère la donnée personnelle comme le support indirect d'un droit fondamental et inaliénable reconnu à l'individu dont elle émane et non comme un objet économique.

b. Consacrer un droit à l'autodétermination informationnelle des individus à l'ère numérique

En lieu et place d'une privatisation de ses données personnelles, la Commission recommande de procéder à une plus grande autonomisation de l'individu dans l'univers numérique, en lui permettant non plus seulement de bénéficier de droits à la protection mais aussi d'être maître de son épanouissement dans l'univers numérique.

L'approche par l'autonomisation individuelle est relativement absente de la législation française, à la différence d'autres pays européens comme l'Allemagne dont la Cour constitutionnelle fédérale a dégagé, dès 1983, des principes de dignité de l'homme et de droit au libre développement de sa personnalité un **droit à l'autodétermination informationnelle** de l'individu. Pour la Cour de Karlsruhe, « *la Constitution* [allemande] *garantit en principe* ***la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel*** » car s'il « *ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est fortement limitée* ». Pour elle, « *l'autodétermination est une condition élémentaire fonctionnelle dans une société démocratique libre, basée sur la capacité des citoyens d'agir et de coopérer* » [(1)].

Le libre épanouissement de la personnalité est un principe présent dans de nombreux États européens, en particulier ceux qui se sont dotés de Constitutions en réaction à des régimes autoritaires (Allemagne, Espagne, Portugal, Italie, etc.). Issu des principes généraux de liberté, de libre arbitre et de libre agir, il sert généralement à limiter la puissance de la loi [(2)] et à prévenir toute violation des droits subjectifs par la puissance publique. En France, la notion de libre épanouissement de la personnalité n'existe pas en tant que telle ; le Conseil constitutionnel a simplement rattaché au principe de liberté protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 plusieurs exigences, parmi lesquelles le droit au respect de la vie privée, l'inviolabilité du domicile privé ou le secret des correspondances [(3)]. Mais, pour reprendre les interrogations formulées par M. Daniel Kaplan au cours de son audition, « *doit-on se contenter de protéger les individus contre l'utilisation que certains acteurs peuvent faire de leurs données ? Les individus ne pourraient-ils pas faire avec leurs données un usage qui aurait du sens pour eux* » ?

---

(1) Traduction en français de l'arrêt du 15 décembre 1983 de la Cour constitutionnelle fédérale de l'Allemagne de Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie. », in État de droit et virtualité, *K. Benyekhlef et P. Trudel (dir.), Montréal : Thémis, 2009.*

(2) L'article 3 de la Constitution italienne dispose que la République a pour objectif fondamental d'« écarter les obstacles d'ordre économique et social qui, en limitant dans les faits la liberté et l'égalité des citoyens, s'opposent au plein épanouissement de la personne humaine *». L'article 10 de la Constitution espagnole dispose que «* la dignité de la personne, les droits individuels qui lui sont inhérents, le libre développement de la personnalité, le respect de la loi et des droits d'autrui sont le fondement de l'ordre politique et de la paix sociale *».*

(3) Voir supra, *le* b *du 1 du A du présent III.*

Pour la Commission, l'individu doit pouvoir disposer de moyens plus importants pour assurer sa protection face aux risques soulevés par le numérique. La prise en compte du libre épanouissement de la personnalité dans notre législation serait de nature à mieux concilier, à l'ère numérique, le respect de la dignité humaine, la préservation de l'intimité et la protection des choix privés dans la sphère publique. Tout en protégeant le noyau de la personnalité, rassemblant les choix de vie et d'identité fondamentaux, elle permettrait l'autodétermination de la personne sur son existence publique, en complément des autres libertés fondamentales dont elle dispose déjà (sûreté, liberté d'aller et venir, liberté d'expression, etc.) (1). En conséquence, la Commission propose de **consacrer dans notre législation un droit à l'autodétermination informationnelle** comme principe directeur des autres droits reconnus par la loi dite « Informatique et libertés ». L'objectif n'est pas de renverser la logique qui a jusqu'alors présidé à l'adoption de règles relatives à la protection des données personnelles mais d'octroyer à l'individu des moyens supplémentaires pour maîtriser la gestion de ses données. Au surplus, une telle consécration présenterait quatre avantages parfaitement résumés par le Conseil d'État (2) :

– elle donnerait sens à tous les autres droits relatifs à la protection des données à caractère personnel qui ne constitue pas un but en soi ;

– « *alors que le droit à la protection des données peut être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu positif (…) à la fois plus efficace et plus conforme à la logique personnaliste et non patrimoniale qui a toujours prévalu en Europe en matière de protection des données* » ;

– elle soulignerait que la législation relative à la protection des données protège non seulement l'individu mais aussi les intérêts collectivement défendus par la société tout entière ;

– elle apparaîtrait « *d'une grande ambition, au regard de la perte générale de maîtrise par les individus de leurs données* » dans un contexte où la donnée personnelle est de plus en plus traitée comme une marchandise.

Recommandation n° 58

En complément de la reconnaissance constitutionnelle des droits au respect de la vie privée et à la protection des données personnelles, consacrer dans notre législation un droit à l'autodétermination informationnelle donnant sens aux droits reconnus à l'individu sur les réseaux numériques.

---

(1) *Xavier Bioy, « Le libre développement de la personnalité en droit constitutionnel : essai de comparaison (Allemagne, Espagne, France, Italie, Suisse) »,* Revue internationale de droit comparé, *vol. 55 n° 1, janvier-mars 2003, pp. 123-147.*

(2) *Conseil d'État,* op. cit., *pp. 264-269.*

Il convient également d'assurer que l'autodétermination informationnelle se traduise par des droits et des moyens supplémentaires [1] pour les individus et ne conduise pas au contraire à les affaiblir dans leurs relations avec les responsables de traitements qui sont généralement dans une position de force par rapport à eux.

C'est pourquoi la Commission appelle l'attention du législateur sur les insuffisances qui naîtraient de la simple inscription de ce droit dans notre *corpus* juridique. Dépourvu de traduction juridique concrète et de moyens techniques effectifs, il ne permettra pas à l'individu de faire face au fonctionnement des réseaux numériques et d'exprimer une volonté éclairée sur la multitude des utilisations de données auxquelles il s'expose plus ou moins volontairement.

C'est pourquoi la Commission estime indispensable d'accompagner cette consécration de mesures plus concrètes tendant à renforcer les droits des personnes, en renouvelant et en adaptant les prérogatives de l'individu dans la société numérique, ainsi que l'a suggéré Mme Isabelle Falque-Pierrotin au cours de son audition du 26 novembre 2014, par « *une quatrième génération de droits, positifs et non pas réactifs* ».

C'est donc un ensemble de droits renouvelés qui devraient donner à l'individu l'autonomie suffisante au libre épanouissement de sa personnalité à l'ère numérique, à travers l'adaptation du principe du consentement préalable au contexte de la collecte des données et l'édiction de nouveaux droits au service de son libre arbitre et de son libre agir. Ces droits devraient être accompagnés, dans l'esprit de la recommandation n° 49, d'outils techniques utilisables par le plus grand nombre, permettant aux individus de mieux appréhender leur environnement numérique en identifiant notamment les possibilités d'accès à leurs données par des tiers ainsi que leur transfert éventuel et leurs conséquences possibles et en leur permettant d'obtenir facilement leur effacement, leur rectification ou leur exportation (portabilité des données).

Parallèlement, la Commission juge nécessaire d'**approfondir les réflexions qui visent à dessiner un principe de « frugalité informationnelle » à l'égard des responsables de traitements**. Cette piste, développée par la Fondation Internet Nouvelle Génération (FING) dans son rapport consacré aux nouvelles approches numériques [2], repose sur l'idée qu'une confiance de long terme entre l'entreprise collectrice de données et l'individu ne peut se construire que sur un dévoilement progressif et maîtrisé de l'individu. À rebours des tendances actuelles qui conduisent les entreprises à chercher à en savoir toujours plus sur l'individu, quitte à se retrouver avec un trop-plein d'informations, il s'agirait pour ces dernières de ne prendre que ce que l'utilisateur accepte de leur donner parce que cela est utile au service qu'elles rendent. Au fur et à mesure que la confiance en l'entreprise s'établit et se renforce, et sans jamais être brusqué, l'individu partagera naturellement de plus en plus d'informations, à proportion et afin de bénéficier de nouveaux services ou avantages pour lesquels ces données

---

(1) Notamment techniques, voir la recommandation n° 49.

(2) FING, Nouvelles approches de la confiance numérique, *février 2011.*

sont utiles. Afin de réduire une asymétrie informationnelle persistante, il est crucial que cette **collecte** s'opère d'une façon **transparente** (mettre l'utilisateur en mesure de savoir les informations dont l'entreprise dispose sur lui) **et réversible** (lui donner la possibilité de revenir sur son consentement, et supprimer effectivement les données collectées le cas échéant). Accompagné de la mise à disposition par l'entreprise collectrice d'un espace ergonomique de gestion des données, ce principe de « frugalité » participerait pleinement pour l'utilisateur d'un droit à l'autodétermination informationnelle.

2. Conserver le principe du consentement préalable de l'individu en l'adaptant au contexte de collecte de ses données

Le consentement préalable figure parmi les conditions de licéité des traitements de données (***a***) mais son impact sur la protection de l'individu est de plus en plus remis en cause par les récents développements technologiques et les usages qui en découlent (***b***). C'est la raison pour laquelle la Commission propose, tout en conservant son principe, d'en revoir la portée normative et les modalités de recueil pour les adapter au contexte de la collecte et du traitement des données (***c***) [(1)].

a. Le consentement préalable est l'une des conditions de licéité d'un traitement

Aujourd'hui, le droit applicable aux traitements de données accorde une grande importance au recueil préalable du consentement de la personne concernée. Aux termes de l'article 7 de la loi dite « Informatique et libertés », la mise en œuvre d'un traitement de données à caractère personnel est conditionnée au **consentement préalable de l'individu**. À défaut, il doit satisfaire à l'une des obligations limitativement énumérées : le respect d'une obligation légale incombant au responsable du traitement ; la sauvegarde de la vie de la personne concernée ; l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ; l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ou la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. L'article 7 de la directive 95/46/CE du 24 octobre 1995 précitée pose des obligations semblables, en exigeant que « *la personne concernée a*[it] *indubitablement donné son consentement* » ou que le traitement soit nécessaire à la réalisation de l'une des cinq conditions énumérées, très proches de celles retenues en droit français [(2)].

---

(1) Voir à ce sujet, en annexe, la contribution écrite de M. Winston Maxwell au groupe de travail sur la vie privée.

(2) « L'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci » *;* « le respect d'une obligation légale à laquelle le responsable du traitement est soumis » *;* « la sauvegarde de l'intérêt vital de la personne concernée » *;* « l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi

Il n'est pas ici question de revenir sur le primat accordé au consentement dans notre législation. La proposition de règlement général sur la protection des données, dans sa version adoptée par le Parlement le 12 mars 2014, ne le remet pas en cause [(1)]. Elle substitue au consentement indubitable un consentement « *pour une ou plusieurs finalités spécifiques* ». Elle exige un accord explicite et éclairé en définissant ainsi la notion de consentement : « *toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Elle renforce également les modalités de son recueil en faisant reposer sur le responsable du traitement la charge de la preuve que la personne concernée a effectivement consenti au traitement, en permettant à celle-ci de retirer son consentement à tout moment et en prévoyant que les traitements de données à caractère personnel relatives à un enfant de moins de 13 ans ne seront licites « *que si et dans la mesure où le consentement est donné ou autorisé par un parent de l'enfant ou par son tuteur légal* ». Pour le reste, elle laisse quasi-inchangées les conditions de licéité tenant à l'exécution d'un contrat, au respect d'une obligation légale, à la sauvegarde des intérêts vitaux de la personne concernée et à l'exécution d'une mission d'intérêt général mais précise celle tenant à la poursuite d'intérêts légitimes [(2)].

b. Les limites du consentement à l'ère numérique

Le consentement peut se heurter, dans l'environnement numérique actuel, à plusieurs limites. « *Les développements technologiques de ces dernières années ainsi que les pratiques sociales qu'ils génèrent semblent battre en brèche la capacité, voire même la volonté, des individus d'exercer un véritable contrôle sur leurs données personnelles* » [(3)] : complexification et sophistication des dispositifs techniques et des modèles commerciaux de collecte des données, sous-estimation par les individus des risques et des dommages potentiels générés par ces traitements de données, opacité ou surformalisation des informations délivrées par les responsables de traitement (recours à des politiques de vie privée ou *privacy policies* longues et complexes), interrogations sur le recueil d'un consentement véritablement libre par ces derniers.

---

le responsable du traitement ou le tiers auquel les données sont communiquées » *;* « la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée ».

(1) Articles 6 à 8 de la proposition de règlement général sur la protection des données.

(2) Le traitement peut être licite s'il est « nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou, en cas de divulgation, par le tiers à qui les données sont divulguées, *», s'«* il satisfait les attentes raisonnables de la personne concernée fondées sur sa relation avec le responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée, qui exigent une protection des données à caractère personnel ».

(3) Christophe Lazaro et Daniel Le Métayer, « Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet », Revue juridique Thémis de l'Université de Montréal, *vol. 48 n° 3, 2014.*

Certains estiment que ce concept de consentement constitue une fiction et qu'il est devenu inadapté au caractère automatisé et massif de la collecte des données. Il convient d'ailleurs de distinguer l'ensemble hétérogène de situations que peut recouvrir la notion générique de consentement – allant de l'accord tacite à la véritable manifestation de volonté – et le consentement véritablement éclairé, qui requiert une information particulière de l'utilisateur, mis en situation de mesurer les conséquences de son choix et d'accepter ou de refuser en toute indépendance le traitement de ses données. Comme l'ont résumé deux chercheurs américains, Mme Ruth R. Faden et M. Tom L. Beauchamp, le consentement éclairé repose à la fois sur l'information, la compréhension, la volonté, la capacité et l'autorisation [(1)]. Or il arrive fréquemment que certains de ces critères ne soient pas réunis au moment de demander l'accord de l'utilisateur pour le traitement de ses données personnelles. Ainsi que l'a indiqué devant la Commission Mme Isabelle Falque-Pierrotin, présidente de la CNIL, « *dans l'univers actuel des données massives, (...) le principe du consentement est moins évident en raison des multiples échanges qui interviennent bien au-delà de la collecte* », rendant de plus en plus illusoire son recueil [(2)].

Sur le plan technique, le consentement informé d'une personne est-il véritablement recueilli lorsqu'un fournisseur de services numériques l'invite à lire et à approuver, par le simple fait de cocher une case, de longues et fastidieuses conditions générales d'utilisation ? Le consommateur le plus attentif et le plus averti pourrait-il même prendre le temps de lire ces conditions d'utilisation et d'apprécier les risques – souvent abstraits à ses yeux – encourus par telle ou telle utilisation de ses données personnelles ? Force est de reconnaître que les conditions ne sont souvent pas réunies pour s'assurer d'un consentement éclairé et réfléchi de la personne concernée. Le consentement de l'individu peut-il être valablement recueilli par d'autres moyens, par exemple des fenêtres *pop-up* ? Il est probable que l'utilisation répétée de telles fenêtres va agacer le consommateur qui, *in fine*, les acceptera systématiquement et ne prêtera plus d'attention à leur contenu [(3)].

Par ailleurs, les fournisseurs de services ne sont généralement pas en mesure d'offrir une alternative au consommateur en cas de refus des conditions d'utilisation de leur site internet. Dans la mesure où un grand nombre de ces services est fourni gratuitement et que le modèle économique des acteurs qui les fournissent est fondé sur la vente de publicités qui requiert l'analyse de données à caractère personnel, le consommateur souhaitant bénéficier de l'un de ces services doit bien souvent en accepter le prix en termes d'utilisation de ses données. Pour compenser le déséquilibre des forces entre les internautes et les fournisseurs de services qui imposent leurs conditions d'utilisation des données personnelles, parfois de manière abusive, il convient de favoriser le développement d'outils et

---

(1) Ruth R. Faden et Tom L. Beauchamp, A history and theory of informed consent, *OUP USA, 1986.*

(2) Audition de Mme Isabelle-Falque-Pierrotin du 26 novembre 2014.

(3) Christophe Lazaro, Daniel Le Métayer, « Control over personal data : true remedy or fairytale ? », Scripted, *vol. 12, n° 1, juin 2015*

de plateformes permettant aux internautes de se regrouper, par exemple pour évaluer des politiques de protection de la vie privée, comme c'est déjà le cas avec ToS;DR [1], ou même pour les négocier.

c. *Conserver le principe du consentement préalable en adaptant sa portée normative et les modalités de son recueil au contexte de la collecte et du traitement des données*

Malgré la validité des arguments empiriques et juridiques qui en relativisent la portée, le consentement demeure, dans son principe, pertinent. Essentiel à la confiance que portent les individus dans la société numérique, « *le rôle du consentement de la personne ne doit être ni surestimé (dans la législation actuelle, il n'est ni une condition nécessaire ni une condition suffisante de la licéité du traitement des données), ni méconnu, car il incarne la liberté de la personne en matière d'utilisation de ses données personnelles* » [2]. Mais sa portée normative peut se trouver amoindrie ou relativisée lorsqu'il est trop systématiquement exigé ou uniformément recueilli, ce qui conduit à abaisser la vigilance des internautes et ne permet pas à l'intéressé d'apprécier l'importance qu'il devrait lui accorder.

Dès lors, si la Commission souhaite que le consentement demeure l'une des conditions fondamentales de licéité des traitements de données personnelles, elle propose de mieux en contextualiser les modalités de recueil afin de les adapter à la nature et à l'étendue de la collecte et du traitement des données, en écartant toute contractualisation du consentement ou marchandisation du droit à la protection des données personnelles. Elle s'est inspirée des nombreuses réflexions menées sur le sujet, notamment d'universitaires [3], et du rôle reconnu au consentement de l'individu par le législateur dans d'autres domaines sensibles, comme en matière médicale et en droit des contrats (voir l'encadré ci-après).

Le consentement en droit médical et en droit des contrats

Après avoir évoqué le rôle qu'occupait le consentement en droit médical et en droit des contrats, MM. Christophe Lazaro et Daniel Le Métayer dressent le constat suivant pour le consentement au traitement des données personnelles : « *dans cette contribution, nous avons essayé d'évaluer la légitimité et l'acceptabilité de la théorie du consentement en matière de protection de la vie privée et des données personnelles. Dans cette perspective, nous avons déployé une analyse comparative en nous inspirant des réflexions critiques suscitées par la notion de consentement dans le champ du droit médical et du droit des contrats. Sur la base de cette comparaison, la grille de lecture que nous avons dressée a permis d'identifier un ensemble de paramètres fondamentaux s'imposant comme des balises dans toute discussion sur la notion de consentement : (1) les rapports de force entre parties, (2) la possibilité de révoquer le consentement, (3) la nature routinière ou exceptionnelle des*

---

(1) Voir supra, *le* a *du 3 du A du présent III.*

(2) Conseil d'État, op. cit., *p. 18.*

*(3) Il s'agit à la fois de travaux d'universitaires comme ceux d'Helen Nissenbaum (« Privacy as contextual integrity », 2004) ou de Frederik J. Zuiderveen Borgesius (« Consent to behavioural targeting in european law - What are the policy implications of insights from behavioural economics ? », 2013), du Forum économique mondial (*Unlocking the value of personal data : from collection to usage, *février 2013) ou du G29 (opinion 03/2013 on purpose limitation, adoptée le 2 avril 2013).*

circonstances, et (4) l'impact du consentement. La prise en compte de ces paramètres permet de se départir d'une conception binaire du consentement en envisageant celui-ci au sein d'un continuum *allant des situations les plus favorables aux plus défavorables* (1)*. En matière de données personnelles, on s'aperçoit que, dans certaines situations, le consentement peut présenter tous les caractères « aggravants » des paramètres susmentionnés. Mais une absence totale de légitimité du consentement semble difficile à envisager dans les situations les plus courantes.*

« *Notre grille de lecture montre qu'il importe donc d'adopter une position nuancée en matière de consentement en tenant compte, autant que possible, de la diversité des situations de traitement de données. Afin de garantir la légitimité du consentement, il conviendrait, par exemple, de distinguer les cas où le consentement pourrait être librement donné et couvert par des règles sanctionnant* a posteriori *les vices dont il serait affecté ; les cas où le consentement pourrait être donné à condition d'être assorti des garanties strictes ; et enfin, les cas où le consentement ne pourrait jamais être donné* (2)*. Une telle approche permet d'insister sur la nécessité de déployer une diversité de règles ou d'instruments normatifs afin d'assurer la protection des données personnelles et de la vie privée* ».

(1) Celles qui se caractérisent par un déséquilibre significatif entre les parties, dans lesquelles la possibilité de révoquer le consentement n'existe pas, dont l'impact est majeur sur le bien-être individuel ou collectif et qui procèdent de circonstances ou d'activités exceptionnelles.

(2) Cette distinction s'inspire de celle propose par The Future of Privacy Forum, op. cit., *pp. 5-6.*

Source : Christophe Lazaro et Daniel Le Métayer, « Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet », Revue juridique Thémis de l'Université de Montréal, *vol. 48 n° 3, 2014.*

La Commission recommande donc de **substituer à l'actuelle logique formelle de recueil du consentement une approche fondée sur la contextualisation en adaptant sa portée normative et les modalités de son recueil en fonction de cinq critères** :

– le **contexte de la collecte des données personnelles** : le **consentement implicite** de l'individu serait considéré comme acquis pour un traitement découlant naturellement du contexte d'origine de la collecte des données pour lequel un premier consentement informé aurait été recueilli ; en revanche, son **consentement explicite** serait exigé dès lors que le traitement sortirait de ce contexte ;

– les **usages auxquels les données collectées sont vouées** : un **consentement renforcé**, par exemple sous la forme de trois clics de souris, d'un appel téléphonique ou de l'envoi d'une lettre ou d'un mail, devrait être exigé pour certains usages qui sortent de l'ordinaire ou présentent une sensibilité particulière ; pour certains types de traitement, le législateur pourrait imposer une **interdiction totale** (1), comme c'est le cas, en France, pour les traitements de données ADN en dehors de la recherche médicale ;

– les **rapports de force entre les parties** : la portée juridique du consentement serait en conséquence réduite en présence d'un **déséquilibre manifeste ou significatif** (2), sous réserve que les motifs de ce déséquilibre soient

---

(1) Frederik J. Zuiderveen Borgesius, « Consent to behavioural targeting in european law - What are the policy implications of insights from behavioural economics ? », 2013.

(2) Le 4 de l'article 7 de la proposition initiale de règlement prévoyait que « le consentement ne constitue pas un fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif entre la

précisément et préalablement définis, à l'instar de ce qui existe déjà en matière de définition des clauses abusives ;

– les **circonstances d'expression et de recueil du consentement** (nature routinière ou exceptionnelle) : ainsi, dans **certaines situations répétitives ou banales**, l'existence du consentement pourrait être déduite implicitement sans exiger une manifestation explicite de volonté ;

– **l'impact du consentement** non seulement **sur la personne qui l'exprime**, qui s'expose à des risques de violation de ses données, mais aussi **sur les tiers** (amis, famille) indirectement exposés aux mêmes risques et **sur les valeurs et intérêts protégés par la société**.

Recommandation n° 59

Passer d'une logique formelle de consentement préalable à une logique de recueil d'un consentement adapté au contexte de la collecte et du traitement des données personnelles (contexte, usages, rapports de force, circonstances de recueil, impact du consentement).

La Commission n'ignore pas les difficultés juridiques et pratiques soulevées par cette proposition. Elle suppose la définition précise mais suffisamment souple et évolutive des conditions susceptibles d'alléger ou de renforcer les formalités relatives au recueil du consentement (contexte, usages, rapports de force, circonstances, impact du consentement). Cette tâche pourrait être confiée au régulateur, familier de ce type d'exercice puisque la CNIL élabore déjà des normes simplifiées ou des autorisations uniques pour certains traitements, définissant ainsi une zone de traitement acceptable à l'intérieur de laquelle le consentement individuel n'est généralement pas nécessaire.

3. Reconnaître à l'individu de nouveaux droits au service de son libre arbitre et de son libre agir

Si, comme elle l'a précédemment évoqué, la Commission n'entend pas revenir sur les droits et principes édictés par la loi dite « Informatique et libertés », elle souhaite cependant restaurer la souveraineté de l'individu sur ses données et réparer l'asymétrie informationnelle et décisionnelle qui caractérise sa relation avec les responsables de traitements. Pour ce faire, elle propose de renforcer l'effectivité des droits reconnus à l'individu afin d'en faire de véritables droits positifs et plus seulement défensifs ou formels (**a**). Elle suggère également de mieux encadrer les algorithmes à caractère décisionnel ou prédictif qui peuvent priver l'individu de son pouvoir d'appréciation et de décision (***b***). Enfin, elle recommande de créer de nouveaux moyens juridiques pour faire cesser les violations de la législation sur les données personnelles (***c***).

---

personne concernée et le responsable du traitement » [(2)] *caractérisé par la situation dans laquelle la personne concernée se trouve dans une relation de dépendance par rapport au responsable du traitement. Cette disposition, relativement imprécise quant au champ des situations qu'elle était susceptible de concerner, a toutefois été supprimée par le Parlement européen.*

a. Renforcer l'effectivité des droits reconnus à l'individu

La Commission formule plusieurs propositions tendant à renforcer l'effectivité des droits aujourd'hui reconnus à l'individu.

De prime abord, le droit pourrait préciser que les données collectées doivent être traitées d'une manière qui permette à la personne concernée d'exercer effectivement ses droits. Ce principe pourrait s'ajouter à la liste des principes régissant déjà les traitements de données personnelles, ainsi que l'envisage la proposition de règlement général sur la protection des données dans sa version adoptée par le Parlement européen le 12 mars 2014 [(1)]. Il pourrait se traduire par des recommandations des autorités de protection des données sur les méthodes ou les techniques disponibles qui devraient être utilisées par défaut par les responsables de traitements pour rendre ces droits effectifs.

Cette exigence d'effectivité a vocation à s'appliquer à l'ensemble des droits reconnus à l'individu par notre législation.

La Commission souhaite qu'elle concerne le droit à être informé des caractéristiques du traitement de données, condition essentielle à l'expression d'un consentement éclairé et à l'autodétermination informationnelle de l'individu dans un univers numérique marqué par la complexité croissante des technologies utilisées et des terminologies employées pour les décrire. Toute personne devrait en effet pouvoir connaître de manière transparente et non biaisée les caractéristiques et les conditions de mise en œuvre d'un traitement de données. Or ce droit s'applique aujourd'hui trop diversement, sous des formats tantôt élémentaires ou superficiels, tantôt obscurs ou compliqués, empêchant la personne concernée d'être parfaitement renseignée et éclairée sur les conséquences de ses choix.

C'est pourquoi la Commission estime indispensable de **renforcer les garanties entourant le droit à l'information** sur le traitement mis en œuvre, en exigeant que **les informations fournies** par le responsable du traitement soient **aisément compréhensibles, claires, visibles et facilement accessibles par les consommateurs**. Les articles 13 *bis* et 14 de la proposition de règlement général sur la protection des données, dans sa rédaction adoptée par le Parlement européen le 12 mars 2014, ouvrent à cet égard des pistes intéressantes, en définissant des « *politiques d'information normalisées* » et en établissant une liste des éléments à fournir à la personne (identité et coordonnées du responsable du traitement, finalité du traitement, informations sur la sécurité et le traitement des données collectées, éléments relatifs à la durée de leur conservation, possibilité de faire valoir certains droits à l'égard du traitement, destinataires des données, etc.).

---

(1) e bis*) de l'article 5 de la proposition de règlement général sur la protection des données.*

Recommandation n° 60

Inscrire dans la loi que les données doivent être traitées d'une manière qui permette à la personne concernée d'exercer effectivement ses droits (principe d'effectivité), en particulier par le biais d'internet lorsque c'est envisageable ;

Conforter l'effectivité du droit à l'information en exigeant que les renseignements fournis à la personne soient accessibles, lisibles et formulés dans un langage compréhensible par le plus grand nombre. À cette fin, encourager la constitution de formats normalisés pour la présentation de ces informations (canevas ou conditions standard d'utilisation des données personnelles par exemple).

Le principe d'effectivité doit également s'appliquer au consentement qui ne doit pas être seulement une fiction mais permettre à l'individu de choisir librement de donner ou de retirer son accord pour le traitement de ses données. À cette fin, la Commission suggère que la personne concernée :

– dispose d'une véritable **solution de rechange** et puisse choisir librement d'accorder ou non son consentement à la collecte et au traitement de ses données, grâce à la mise à disposition d'une **offre réellement neutre** (services non personnalisés par exemple) ;

– puisse révoquer à tout moment son accord en faisant valoir un **droit au retrait du consentement** : cette proposition nécessitera toutefois de réfléchir plus concrètement aux conséquences qu'aura la rétractation ou la révocation du consentement sur la délivrance du service en cours et l'effacement des données déjà collectées.

Recommandations n°s 61 et 62

Afin de renforcer l'effectivité du consentement :

– n° 61 : prévoir que la personne bénéficie d'une solution de rechange si elle ne souhaite pas que ses données fassent l'objet d'une collecte et d'un traitement ;

– n° 62 : instaurer un droit au retrait du consentement.

Par ailleurs, la Commission s'est interrogée sur l'adéquation des droits traditionnels d'opposition [(1)], de rectification et d'effacement [(2)] à l'émergence des moteurs de recherche qui permettent aujourd'hui de rassembler et de conserver l'ensemble des informations se rapportant à un individu, sur une durée presque illimitée, sans faire le tri entre celles qui mériteraient toujours d'être référencées et celles qui ne devraient plus l'être.

---

(1) Article 38 de la loi n° 78-17 du 6 janvier 1978 précitée.

(2) Article 40 de la loi n° 78-17 du 6 janvier 1978 précitée.

Comme l'a indiqué Mme Marie Mongin, vice-présidente de la 17e chambre du tribunal de grande instance de Paris, auditionnée le 3 juillet 2014, « *face à la mémoire qu'offre internet et qui dépasse les capacités humaines, se pose (...) de manière croissante la question du droit à l'oubli. Jacques Fauvet disait que l'oubli est le fruit de la faiblesse humaine. Or, avec internet, il n'y a plus la faiblesse humaine pour permettre cet oubli. Pour faire face à une mémoire qui n'a plus de faille et qui est éternelle, pour faire face à des moteurs de recherche qui permettent de retrouver toute information, toujours et en tout lieu, le droit est en train d'inventer cette notion, qui vient apporter des limites à la liberté d'expression* ».

Pour tenir compte de cette situation, la CJUE a, en 2014, dans l'arrêt *Google Spain c. AEPD*, jugé que toute personne avait, sous certaines conditions, un droit au déréférencement des informations la concernant. Elle a estimé que l'activité de référencement des moteurs de recherche, considérés comme des responsables de traitements de données personnelles, était « *susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel* » en permettant « *à tout internaute d'obtenir par la liste de résultats un aperçu structuré des informations relatives à* [une] *personne trouvables sur Internet, qui touchent potentiellement à une multitude d'aspects de sa vie privée* » (1). Pour juger de la légalité d'une telle ingérence, elle invite à confronter l'intérêt économique du moteur de recherche, l'intérêt de la personne concernée à voir ses données effacées et l'intérêt légitime des internautes à avoir accès à ces informations. Elle indique que l'intérêt de la personne concernée doit être apprécié en fonction de la nature de l'information en cause, de sa sensibilité pour la vie privée et « *du rôle joué par cette personne dans la vie publique* » (2) : elle considère ainsi que, de manière générale, l'intérêt de la personne concernée prévaut sur l'intérêt du moteur de recherche et des personnes souhaitant avoir accès à ces informations, sauf si la personne joue un rôle tel dans la vie publique que l'intérêt du public à l'information doit prévaloir.

La Commission est bien consciente du changement qu'a constitué l'essor d'internet et des moteurs de recherche, en permettant de rendre les informations publiées à l'égard d'une personne plus accessibles grâce à leur recoupement permanent et sans limitation de temps. Elle préconise donc de renforcer l'effectivité des droits traditionnels d'opposition, de rectification et d'effacement en veillant toutefois à concilier ces droits, nécessaires à la protection de la vie privée, avec les autres libertés fondamentales en jeu, la liberté d'expression et le droit à l'information.

La Commission est **opposée à la reconnaissance d'un « droit à l'oubli »** dans l'univers numérique. Pareil droit conduirait inévitablement à faire disparaître des réseaux des contenus nécessaires au droit à l'information et indispensables à la compréhension de certains événements, notamment historiques. Il impliquerait en

---

(1) CJUE, 13 mai 2014, Google Spain c. Agencia Española de Protección de Datos (AEPD), *n° C-131/12, § 38.*
(2) Ibid, *§ 81.*

effet de procéder non seulement au déréférencement de l'information devenue inappropriée mais également au retrait de la publication de l'information du site dont elle émane, par exemple un site de journalisme.

La Commission est en revanche favorable à ce qu'une personne qui s'estime lésée par le référencement des informations qui la concernent puisse demander la suppression de certains liens apparaissant dans les résultats de recherche effectués sur la base de son nom lorsque les intérêts de la personne prévalent sur les éventuels effets de la mesure sur la liberté d'expression de l'éditeur du site et sur la liberté d'accès à l'information du public. Par exemple, les articles faisant mention de condamnations pénales ne figurant plus au casier judiciaire de la personne ne devraient plus être référencés par les moteurs de recherche. La Commission souligne la nécessité de prévoir l'intervention d'une autorité judiciaire à chaque fois qu'est en cause une liberté individuelle, et notamment la liberté d'expression.

La Commission propose donc de **consacrer le droit au déréférencement** reconnu par la CJUE.

Recommandation n° 63

Consacrer un droit au déréférencement des informations inexactes, incomplètes, équivoques ou périmées apparaissant dans les résultats présentés par les moteurs de recherche.

Elle suggère d'en préciser les conditions d'exercice afin d'encadrer la manière dont les moteurs de recherche le mettent en œuvre, en s'inspirant des lignes directrices déjà édictées par les autorités de régulation européennes (1) et en clarifiant ainsi sa mise en œuvre pratique :

– par l'instauration d'une procédure contradictoire permettant au demandeur, au moteur de recherche et à l'éditeur du site dont le déréférencement est demandé de faire valoir leurs observations ;

– par la faculté pour le demandeur, l'éditeur du site ou le moteur de recherche de saisir un juge en cas de désaccord ;

– par l'attribution de la compétence territoriale pour connaître des litiges relatifs au droit au déréférencement à un nombre limité de tribunaux de grande instance (2) ;

– par la pleine application des procédures de référé, adaptées au traitement des différends en la matière (1) ;

---

(1) Lignes directrices adoptées par les autorités européennes de protection des données réunies au sein du Groupe de l'article 29 (G29) le 26 novembre 2014.

(2) Sur le modèle de l'article R. 442-3 du code de commerce, les juridictions compétentes pourraient être les tribunaux de grande instance des villes suivantes : Marseille, Bordeaux, Lille, Fort-de-France, Lyon, Nancy, Paris et Rennes.

– par l'application du déréférencement à l'ensemble des moteurs de recherche ;

– par la garantie que l'information originale sera toujours accessible en ligne en consultant directement le site source ou en lançant une requête avec d'autres termes.

Les modalités d'application du droit au déréférencement, et notamment son étendue territoriale, doivent obéir au principe de proportionnalité et tenir compte de la nécessité de maintenir un niveau élevé de protection de la liberté d'expression sur internet au niveau mondial. Elles doivent garantir l'effectivité du déréférencement des informations erronées ou datées qui sont publiées à l'égard des internautes français ou européens sans conduire à l'appauvrissement de l'information accessible à ces mêmes internautes à travers les moteurs de recherche [(2)].

Recommandation n° 64

Encadrer ce droit au déréférencement afin de concilier de manière adéquate les droits au respect de la vie privée et à la protection des données personnelles, la liberté d'expression et le droit à l'information.

Enfin, au-delà des droits actuels d'accès et de rectification, la Commission souhaite que l'individu se voie reconnaître la possibilité de s'extraire d'un traitement de données en sollicitant la restitution de ses données. Elle recommande donc d'instituer **un véritable droit à la portabilité de ses données**. Il s'agirait de permettre à une personne d'obtenir une copie exhaustive des données faisant l'objet d'un traitement dans un format électronique couramment utilisé et de pouvoir les réutiliser ultérieurement et librement, y compris dans un environnement technique différent. Cela implique notamment que la restitution des données se fasse dans des formats ouverts et standards – permettant d'être lues par tout type de machine – et de manière complète et non dégradée.

Deux préalables doivent cependant être posés à l'instauration d'un tel droit :

– le concevoir comme un droit non pas seulement individuel mais également communautaire, en réfléchissant à ses modalités d'exercice dans une architecture centralisée où, par exemple, l'individu souhaitant quitter un média ou un réseau social voudrait également partir avec ses relations et contacts ;

– permettre à une entreprise de continuer à utiliser des données non personnelles qu'elle aurait pu générer à partir d'elles afin de ne pas fragiliser la

---

(1) On notera que seules des décisions de référé ont été rendues jusqu'à présent : TGI de Paris (référé), 16 septembre 2014 ; TGI de Paris (référé), 24 novembre 2014 ; TGI de Paris (référé), 8 décembre 2014 ; TGI de Paris (référé), 19 décembre 2014 ; TGI de Toulouse (référé), 21 janvier 2015.

(2) Une loi russe sur le droit à l'oubli est en cours d'adoption : son application extraterritoriale conduirait à limiter l'information disponible pour les internautes français à travers les moteurs de recherche.

chaîne de valeur de l'entreprise en faisant peser sur elle le risque permanent que la personne concernée pourra soustraire à tout moment la valeur tirée de ses données.

Recommandation n° 65

Instituer un droit à la restitution des données collectées aux individus dont elles émanent, dans des formats ouverts et standards et de manière complète et non dégradée (droit à la portabilité des données).

b. Accroître les droits des individus face aux algorithmes

Un nombre croissant d'acteurs du numérique, singulièrement les plateformes, recourt à des algorithmes prédictifs ou à caractère décisionnel, destinés à personnaliser le service rendu à leurs clients ou à fournir des aides à la prise de décision. La présomption d'infaillibilité et d'objectivité associée à ces dispositifs a tendance à déposséder les individus des choix qu'ils peuvent faire et à réduire leur libre arbitre, faisant de ces services non plus de simples mécanismes d'aide à la décision mais de véritables systèmes de décision automatique ou semi-automatique. Ces algorithmes affectent non seulement les droits des consommateurs mais aussi la relation de l'usager et du citoyen avec les pouvoirs publics alors qu'émerge une véritable « action publique algorithmique » destinée, par exemple, à anticiper certains comportements dans le domaine social (aide au diagnostic médical, prédiction des risques de maltraitance, anticipation des risques de décrochage scolaire, etc.) (1) ou en matière de sécurité (2).

Il apparaît donc nécessaire de compléter les droits d'information, d'accès et d'opposition aujourd'hui reconnus à l'individu face au traitement de ses données par un encadrement accru des algorithmes. Si l'article 10 de la loi dite « Informatique et libertés » interdit déjà qu'une décision produisant des effets juridiques à l'égard d'une personne soit prise « *sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* », force est de reconnaître qu'à l'heure de la « gouvernementalité algorithmique » (3), cette interdiction est de moins en moins opérante.

La Commission souhaite **réparer l'asymétrie informationnelle et décisionnelle qui existe entre les personnes qui font l'objet de tels algorithmes et leurs concepteurs et utilisateurs**. Comme le Conseil d'État (4), elle pense que **de nouvelles règles devraient régir le fonctionnement des algorithmes prédictifs**, notamment :

---

(1) Pour plus de précisions, voir Élisabeth Grosdhomme Lulin, Gouverner à l'ère du Big Data. Promesses et périls de l'action publique algorithmique, *Institut de l'entreprise, mai 2015, pp. 27-31.*

(2) Voir infra, *le 3 du C du présent III.*

(3) Voir supra, *le* a *du 1 du A du présent III.*

(4) Conseil d'État, op. cit., *pp. 299-304.*

– un **droit d'opposition au profilage** susceptible de conduire à des mesures produisant des effets juridiques pour la personne concernée ou affectant de manière significative ses intérêts, droits ou libertés, hors les cas dans lesquels le profilage est réalisé en application d'une obligation légale, contractuelle ou après que le consentement éclairé de la personne a été valablement recueilli ;

– une **obligation d'intervention humaine effective** : toute décision prise à l'aide d'un algorithme doit reposer sur l'intervention effective d'une personne au regard de critères précis : marge de manœuvre de la personne décisionnaire par rapport à la décision suggérée par l'algorithme, prise en compte d'autres informations que celles retenues par l'algorithme pour prendre une autre décision, etc. ;

– une **obligation de transparence** sur les données personnelles utilisées par l'algorithme et les modalités de son paramétrage, permettant le cas échéant d'en contester la logique générale ou la véracité des données analysées ;

– l'**interdiction d'utiliser des algorithmes ayant pour effet, directement ou indirectement, d'instaurer une discrimination** fondée notamment sur la race, l'origine ethnique, les opinions politiques, la religion, les convictions, l'appartenance syndicale, l'orientation sexuelle ou l'identité de genre.

Recommandation n° 66

Créer de nouveaux droits pour les individus faisant l'objet d'algorithmes qui peuvent avoir une incidence sur leur vie, notamment les algorithmes prédictifs ou à caractère décisionnel, en instaurant un droit d'opposition au profilage et en les soumettant à des exigences d'intervention humaine effective, de transparence et de non-discrimination.

Par ailleurs, la Commission estime nécessaire le lancement d'une **réflexion à plus long terme sur l'impact de la généralisation de la pratique de la personnalisation et les risques que cette généralisation peut poser sur le plan social**, par exemple en termes de discrimination généralisée – au-delà des critères de discrimination posés de manière limitative par la loi – ou d'uniformisation de la société, de réduction de la liberté de choix des individus ou encore de manipulation, lorsque la personnalisation a pour but d'influencer les comportements.

c. Doter les individus des moyens juridiques de faire cesser un manquement à la législation en matière de protection des données personnelles

La Commission est préoccupée par la faiblesse des dispositions juridiques permettant de faire connaître et cesser les manquements à la législation de certains responsables de traitements.

D'une part, l'établissement de procédures de mise en conformité en continu de leurs activités à la réglementation, l'édiction de règles de responsabilisation de ces acteurs et la mise en place de contrôles réguliers et

approfondis de leurs traitements ne sont pas toujours des garanties suffisantes permettant d'appréhender certaines pratiques illégales ou non conformes aux engagements pris par le responsable du traitement.

C'est la raison pour laquelle la Commission propose d'**instaurer un droit d'alerte des salariés des entreprises traitant des données personnelles leur permettant de signaler des pratiques qu'ils estiment contraires à la réglementation**. Certes il existe déjà de nombreux droits d'alerte spécifiques, un droit d'alerte général protégeant toute personne qui aurait « *relaté ou témoigné, de bonne foi, de faits constitutifs d'un délit ou d'un crime dont il aurait eu connaissance dans l'exercice de ses fonctions* » (1) et les dispositions de l'article 40 du code de procédure pénale dont le second alinéa dispose que « *toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* » (2).

Mais aucun des droits d'alerte spécifiques ne concerne la violation de la législation relative aux données personnelles. Si la plupart des manquements à cette législation, réprimés par les articles 226-16 à 226-24 du code pénal, pourraient être rendus publics sur le fondement du droit d'alerte général, certains ne font pas l'objet d'une incrimination pénale et d'autres peuvent simplement correspondre au non-respect de règles déontologiques et de bonne conduite que le responsable du traitement s'est lui-même publiquement fixées pour s'attirer la confiance des consommateurs. Un tel droit d'alerte serait d'autant plus nécessaire si la législation relative à la protection de la vie privée s'orientait vers une responsabilisation accrue des responsables de traitements et une logique de respect en continu des règles qu'elle a posées. La Commission estime que la CNIL pourrait être la destinataire de ces signalements, après le filtre du délégué à la protection des données s'il en existe un ou directement devant elle lorsque tel n'est pas le cas. Ces signalements devraient pouvoir être effectués par l'intermédiaire de mécanismes et de canaux sécurisés, présentant toutes les garanties nécessaires à la protection du lanceur d'alerte.

Recommandation n° 67

Instaurer devant la CNIL un droit spécifique d'alerte pour les salariés des entreprises traitant des données personnelles qui souhaitent signaler des pratiques contraires à la législation ou non-conformes aux engagements pris par le responsable du traitement.

D'autre part, il importe de permettre aux individus de faire valoir leurs droits en saisissant la justice afin que le manquement à la législation cesse rapidement. Si, en principe, toute personne qui s'estime lésée par un traitement

---

(1) En application du premier alinéa des articles L. 1132-3-3 du code du travail et 6 ter *de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.*

(2) Pour plus de précisions, voir supra, *le 1 du C du I.*

contrevenant à la réglementation peut saisir individuellement un juge, en pratique le nombre de recours individuels est faible, principalement en raison du caractère limité du préjudice subi par la personne et de la difficulté à en apprécier les conséquences à plus long terme. C'est souvent le nombre de personnes affectées par un manquement ou une faille de sécurité qui peut encourager l'individu à porter plainte.

La Commission souhaite donc renforcer les capacités d'action collective en matière de protection des données personnelles. Un premier pas a été franchi par le législateur en 2014 (1) lorsqu'il a créé une procédure d'action de groupe visant à la « *réparation des préjudices patrimoniaux résultant des dommages matériels subis par les consommateurs* » (2), y compris dans des litiges intéressant la protection des données personnelles. Mais tous les préjudices liés à la protection des données personnelles ne sont pas patrimoniaux et ne s'inscrivent pas dans une relation contractuelle commerciale entre des consommateurs et un responsable de traitements. Résultant d'une atteinte à l'une des composantes de la vie privée, ils sont d'ailleurs souvent moraux. De plus, les personnes concernées cherchent moins à réparer leur éventuel préjudice qu'à faire cesser la violation de la législation. La proposition de règlement général sur la protection des données, dans sa rédaction adoptée par le Parlement européen le 12 mars 2014, prévoit également d'instaurer un recours collectif en cas de violation des règles de protection des données personnelles, ouvert à tout organisme, organisation ou association agissant dans l'intérêt du public. Mais ce recours, qui s'exercerait auprès d'une autorité de contrôle, ne serait pas juridictionnel (3).

La Commission propose d'aller plus loin que le droit existant et que la proposition formulée par le législateur européen. Elle suggère de **créer une action collective permettant à des groupements de consommateurs et à des associations de défense de la vie privée et des données personnelles préalablement agréés, ainsi qu'à des organisations syndicales pour les traitements de données des salariés d'une entreprise, de former un recours devant le juge judiciaire tendant à faire cesser la violation de la législation, le cas échéant sous astreinte**. Cette faculté est déjà possible pour les traitements mis en œuvre par les personnes publiques par le biais du référé-liberté ou du recours pour excès de pouvoir qui peuvent être formés devant le juge administratif et assortis de demandes d'injonction.

Recommandation n° 68

Créer une action collective destinée à faire cesser les manquements à la législation sur les données personnelles, ouverte à certains groupements, associations et syndicats présentant un intérêt à agir.

---

(1) Loi n° 2014-344 du 17 mars 2014 relative à la consommation.

(2) Articles L. 423-1 et L. 423-2 du code de la consommation.

(3) Article 73 de la proposition de règlement général sur la protection des données.

C. CONFORTER LA PROTECTION DE LA SPHÈRE PRIVÉE À L'HEURE DE LA SURVEILLANCE INSTITUTIONNELLE

Les droits au respect de la vie privée et à la protection des données personnelles ne sont pas seulement affectés par l'utilisation du numérique par les acteurs privés. Ils sont également fragilisés par l'usage que font les personnes publiques des technologies mises à leur disposition. C'est particulièrement vrai de l'utilisation du numérique par l'autorité administrative, dont la mission est de sauvegarder l'ordre public, et par l'autorité judiciaire, qui a pour tâche « *de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs* » (1).

La Commission a été plus particulièrement interpellée par les révélations d'Edward Snowden sur les programmes de surveillance de masse mis en œuvre par les États-Unis et a eu l'occasion de se prononcer sur deux projets de loi examinés par le Parlement tendant à renforcer les dispositions relatives à la lutte contre le terrorisme (2) et à doter la France d'un nouveau cadre juridique pour ses services de renseignement (3).

Dans ce contexte, la Commission a souhaité formuler plusieurs recommandations destinées à mieux encadrer l'activité des pouvoirs publics à l'ère numérique, afin de trouver un juste équilibre entre, d'une part, les nécessités constitutionnelles de préservation de l'ordre public, et, d'autre part, les droits de chacun au respect de sa vie privée, de sa correspondance, de son domicile et de ses données personnelles. Devant l'ampleur des questions qui se posaient, la Commission s'est concentrée sur les principales nouvelles techniques de renseignement et d'investigation permises par les dernières évolutions technologiques. Sans méconnaître certaines des difficultés qu'elles peuvent aujourd'hui soulever, elle n'a donc pas examiné les questions intéressant les fichiers de sécurité ainsi que la vidéosurveillance et la vidéoprotection, modes opératoires anciens dont le numérique a seulement renforcé l'efficacité, dans le premier cas, en améliorant la conservation et les possibilités de comparaison des données collectées et, dans le second cas, en facilitant la conservation et l'exploitation des images grâce au passage de l'analogique au numérique. Ces questions ont d'ailleurs déjà fait l'objet de nombreuses analyses et recommandations de la part du Parlement (4), du Conseil d'État (5) ou de la CNIL (6).

---

(1) Article 14 du code de procédure pénale.

(2) Voir les recommandations des 22 juillet et 29 septembre 2014 sur plusieurs articles du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme.

(3) Voir la recommandation du 1er avril 2015 sur le projet de loi relatif au renseignement.

(4) Sur les fichiers de sécurité, voir les rapports d'information de Mme Delphine Batho et M. Jacques-Alain Bénisti au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers de police (n° 1548, XIIIe législature, mars 2009) et sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police (n° 4113, XIIIe législature, décembre 2011).

(5) Sur les fichiers de sécurité, voir par exemple : Conseil d'État, op. cit., *pp. 314-318.*

(6) Sur les fichiers de sécurité, voir : CNIL, Rapport d'activité 2012, *« TAJ : un nouveau fichier d'antécédents pour remplacer le STIC et le JUDEX », pp. 22-23. Sur la vidéosurveillance et la vidéoprotection, voir : CNIL,* Rapport d'activité 2012, *« Vidéosurveillance / vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée », pp. 40-41 et* Rapport d'activité 2013, *« Vidéoprotection : bilan de trois ans de contrôles », pp. 56-58.*

Après avoir constaté que notre législation était insuffisamment protectrice des droits et libertés fondamentaux eu égard aux conditions dans lesquelles se déroulent aujourd'hui les activités de surveillance institutionnelle, à des fins de police administrative ou judiciaire (**1**), la Commission souhaite que les droits de chacun au respect de sa vie privée et à la protection de ses données soient parfaitement garantis, en instaurant pour les activités de renseignement un régime juridique global, cohérent et respectueux des libertés (**2**) et en encadrant davantage les nouveaux moyens d'investigation des services de police et de justice (**3**).

1. Des règles inadaptées à la protection des droits fondamentaux à l'ère numérique

Au fil de ses auditions et réflexions, la Commission a dressé le constat de l'insuffisance et de l'inadaptation des règles encadrant les activités de surveillance institutionnelle, compte tenu de la faiblesse du cadre juridique applicable aux activités de renseignement (***a***) et de la redéfinition des prérogatives des services de police et de justice permise par le numérique (***b***).

a. La faiblesse du cadre juridique applicable aux activités de renseignement

Les récentes évolutions technologiques ont bouleversé les conditions d'exercice des activités de renseignement à l'ère numérique. Au moment où les réseaux numériques ont pris une place importante dans la vie des individus, un nombre croissant d'outils technologiques de plus en plus perfectionnés et intrusifs facilite leur exploration par les autorités publiques sans qu'ait été défini un cadre juridique adapté qui en précise les conditions d'utilisation. La Commission reviendra ultérieurement sur le cadre proposé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement [(1)].

Plusieurs personnalités auditionnées par la Commission ont estimé qu'il n'existait pas, à ce stade, en France, d'espionnage massif et multiforme de la part des services de renseignement. Comme l'a indiqué devant elle, le 13 novembre 2014, M. Jean-Jacques Urvoas, qui présidait alors la délégation parlementaire au renseignement, la France pratique la « *pêche au harpon* » là où d'autres pays pratiquent la « *pêche au chalut* ». M. Jean-Marie Delarue, alors président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), a également estimé que la surveillance – telle qu'il a eu à la connaître – « *n'est pas généralisée, mais ciblée* », tout en soulignant les faiblesses et les insuffisances du cadre juridique et des moyens de contrôle des techniques de renseignement. Pour M. Jean-Jacques Urvoas, une surveillance massive n'est ni dans la culture philosophique et juridique, ni dans les moyens des services de renseignement français, et ce, pour au moins quatre raisons. En premier lieu, la France se veut, dans ce domaine, une puissance souveraine en n'appartenant pas aux *Five Eyes*, cercle de mutualisation des moyens de renseignement réunissant

---

(1) Voir infra, *le 2 du présent C.*

les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. En deuxième lieu, là où les États-Unis et le Royaume-Uni ont développé une confiance aveugle dans le renseignement technique – le *Government Communications Headquarters* (GCHQ) britannique compte six mille spécialistes de l'écoute – la France a maintenu une préférence pour le renseignement humain, en raison de sa situation géographique outre-mer et de ses zones d'influence privilégiées. En troisième lieu, le cadre juridique dans lequel les services français évoluent est traditionnellement plus restrictif qu'aux États-Unis. En dernier lieu, la France n'a pas les moyens d'une telle surveillance, comme en témoigne le budget de la *National Security Agency* (NSA), l'une des seize agences de renseignement américaines, cinquante fois supérieur à celui de la direction générale de la sécurité extérieure (DGSE).

Toutefois, l'état du droit et l'évolution des technologies ne permettent pas d'écarter l'hypothèse d'une surveillance massive et généralisée. Au cours de son audition du 13 novembre 2014, M. Jean-Marc Manach, journaliste spécialiste des questions de surveillance et de vie privée sur internet, a relativisé le caractère ciblé de la surveillance administrative en évoquant le recours à plusieurs technologies comme les dispositifs techniques de proximité (*IMSI-catchers*) qui, semblables à des cellules téléphoniques, permettent d'intercepter les numéros de tous les utilisateurs situés dans leur zone et, pour les plus sophistiqués, de capter des SMS, le contenu de conversations et le trafic internet, les balayages de ports (*port scanning*) ou les enregistreurs de mots de passe ou de frappe (*keyloggers*). MM. Tobias Engel et Karsten Nohl, deux chercheurs en sécurité, ont également mis en lumière à la fin du mois de décembre 2014 les failles de sécurité qui affectent le réseau SS7, réseau interne aux opérateurs de téléphonie mobile, permettant, en dehors de tout cadre juridique, à des agences de renseignement de procéder à la localisation des utilisateurs de téléphones mobiles et à l'interception de leurs appels et SMS [(1)]. L'ampleur de la surveillance administrative dépend aussi de la surveillance opérée par les services de renseignement sur les contenus publics et semi-publics présents sur les réseaux sociaux comme *Facebook* et *Twitter*.

Dans ce contexte, la Commission regrette l'absence, en France, de culture démocratique des activités de renseignement, résultat selon elle de l'imbrication des pouvoirs chargés de les contrôler, du secret excessif qui entoure l'audition des responsables des services de renseignement et de l'opacité des liens qui existent entre les services français et certaines sociétés privées impliquées dans des activités de renseignement (interrogations sur le rôle de *Qosmos* en Syrie et d'*Amesys* en Libye). De manière plus préoccupante encore, la France s'est longtemps contentée d'un cadre juridique incomplet et minimaliste, avant que le législateur se décide, en 2015, à définir dans sa globalité un régime juridique

---

(1) Craig Timberg, « For sale: Systems that can secretly track where cellphone users go around the globe », The Washington Post, *24 août 2014 ; Martin Untersinger, « Le SS7, le réseau des opérateurs qui permet de surveiller vos téléphones portables »,* Pixels, *Lemonde.fr, 29 décembre 2014.*

applicable aux activités de surveillance administrative, mais sans apporter des garanties suffisantes [1].

Dépourvues de base légale avant 1991, les écoutes administratives – comme les interceptions judiciaires – ont été encadrées par la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances, votée à la suite de la condamnation de la France par la CEDH [2]. Cette loi s'articulait autour de cinq piliers :

– la protection du secret de toutes les correspondances et des communications électroniques [3] ;

– la définition des motifs susceptibles de justifier qu'il soit porté atteinte à cette protection : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité organisée et de la reconstitution ou du maintien de groupements dissous [4] ;

– la compétence du Premier ministre pour décider de procéder à l'interception de correspondances par une décision écrite et motivée [5] ;

– la limitation du nombre [6] et de la durée d'autorisation de l'interception [7] et de conservation des enregistrements des écoutes [8] ;

– et l'autorisation de la transcription des seuls enregistrements ayant reçu une autorisation, les enregistrements touchant à la vie privée ne pouvant être conservés lorsqu'ils ne sont plus indispensables à la réalisation de ces finalités.

Elle complétait ce dispositif par la création d'une autorité administrative indépendante, la CNCIS, chargée de veiller au respect de ces dispositions, les décisions motivées du Premier ministre lui étant communiquées en principe dans les 48 heures. En 2004, le champ des communications concernées a été étendu au-delà des seules écoutes téléphoniques pour inclure l'ensemble des communications électroniques [9].

Vingt-trois ans après son adoption, l'équilibre de la loi de 1991 a toutefois été rompu. La société est devenue à la fois plus sensible au besoin de sécurité – le

---

(1) Voir infra, *le 2 du présent C.*

(2) Voir infra, *le* b *du présent 1.*

(3) Article L. 241-1 du code de la sécurité intérieure.

(4) Articles L. 241-1 et L. 241-2 du même code.

(5) Article L. 242-1 du même code.

(6) Article L. 242-2 du même code : le contingent n'est pas annuel mais peut être augmenté après avis de la CNCIS. Fixé à 1 180 en 1991, il a été successivement porté à 1 840 en 2009 puis 2 190 en 2014.

(7) Article L. 242-3 du même code.

(8) Article L. 242-6 du même code.

(9) Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

droit à la sécurité fut reconnu par la loi en 1995 [1], donc postérieurement à celle relative aux interceptions – et est exposée à de nouvelles menaces terroristes ainsi qu'à l'essor de la criminalité internationale. Parallèlement, les moyens de communication se sont considérablement développés, conduisant les services à déployer de nouvelles méthodes intrusives, pas toujours encadrées et n'offrant pas de garanties suffisantes aux citoyens.

Le législateur est progressivement intervenu pour élargir le spectre des données susceptibles d'être saisies par les services de renseignement bien au-delà des seules écoutes téléphoniques. En 2006 [2], pour les besoins de la lutte contre le terrorisme, il a créé une nouvelle procédure de réquisition administrative des données techniques de connexion ou métadonnées (identification des personnes utilisatrices du service, destinataires des communications, durée, localisation des équipements terminaux, etc.) auprès des fournisseurs d'accès à internet et des hébergeurs [3]. La mise en œuvre de cette procédure a été placée sous le contrôle d'une personnalité qualifiée [4], la CNCIS étant simplement informée des réquisitions et compétente pour formuler, *a posteriori*, des recommandations [5].

En 2013, la loi de programmation militaire [6] a modifié le régime juridique applicable à cette procédure, notamment en élargissant ses motifs pour les aligner sur ceux applicables à l'interception de communications. La rédaction retenue par son article 20 a soulevé d'importantes inquiétudes sur le champ des données susceptibles d'être réquisitionnées, en autorisant « *le recueil (…) des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques* » [7], laissant imaginer qu'était également autorisé un accès aux données de contenu et non plus seulement aux données de connexion [8]. Par la même loi, le législateur a aussi autorisé le recueil en temps réel de ces mêmes informations (géolocalisation en temps réel notamment) mais a soumis cette possibilité, qu'il a jugée intrusive et susceptible de porter atteinte à la liberté d'aller et de venir, au même régime juridique que celui qui s'applique aux interceptions de sécurité [9].

---

(1) L'article 1er de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité disposait que « la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives ». *Cette disposition figure désormais à l'article L. 111-1 du code de la sécurité intérieure.*

(2) Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

(3) Article L. 246-1 du code de la sécurité intérieure.

(4) Article L. 246-2 du même code.

(5) Article L. 246-4 du même code.

(6) Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

(7) Article L. 246-1 du même code.

(8) Dans sa décision n° 2015-478 QPC du 24 juillet 2015, le Conseil constitutionnel a toutefois jugé que les données recueillies dans ce cadre ne pouvaient porter sur le contenu de correspondances ou les informations consultées en se fondant sur la définition donnée par les articles L. 34-1 du code des postes et des communications électroniques et 6 de la LCEN à la notion de données traitées ou conservées par les réseaux ou services de communications électroniques.

(9) Article L. 246-3 du code de la sécurité intérieure.

En définitive, le cadre juridique applicable aux activités de surveillance administrative apparaît principalement fondé sur la distinction entre certaines techniques de renseignement jugées particulièrement intrusives, justifiant l'existence de règles plus strictes et de contrôles renforcés, et d'autres techniques réputées ne pas soulever les mêmes dangers pour la protection de la vie privée, soumises à un régime juridique allégé.

La Commission estime que la pertinence de cette distinction doit être relativisée car, à l'ère numérique, les collectes des métadonnées ne sont pas anodines et peuvent parfois être plus intrusives que l'accès au contenu des données elles-mêmes. Comme l'a souligné M. Jean-Marie Delarue devant elle, « *la saisie répétitive et portant sur des domaines étendus de métadonnées apporte beaucoup d'informations, d'autant plus précieuses que ceux qui pensent être l'objet d'interceptions de sécurité sont discrets dans leurs propos* ». La réputation de plus faible intrusion des métadonnées dans la vie des individus n'est plus totalement convaincante : en conséquence, « *il convient de* ***considérer toute saisie d'information sur la vie personnelle de manière uniforme*** ».

b. La redéfinition des prérogatives des services de police judiciaire et administrative

Le numérique tend aussi à renforcer l'efficacité des moyens mis à la disposition des services de police et de justice pour l'accomplissement de leurs missions en leur permettant d'employer de nouvelles techniques spéciales d'investigation. Même s'ils touchent à des prérogatives essentielles au maintien de la sécurité et à la préservation des atteintes à l'ordre public, ces moyens ne doivent pas déposséder l'individu de tous ses droits ni être utilisés sans garanties.

Certains de ces outils ont d'ores et déjà fait l'objet d'un encadrement par le législateur, comme les modalités de surveillance judiciaire du contenu des communications ou de leurs caractéristiques techniques et la géolocalisation judiciaire.

Avant 1991, les écoutes judiciaires pratiquées sur commission rogatoire étaient mises en œuvre sur le fondement de l'article 81 du code de procédure pénale, aux termes duquel « *le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité* ». L'imprécision de cette disposition ne satisfaisant pas à l'exigence de prévisibilité de la loi posée par l'article 8 de la CESDH [(1)], la loi n° 91-646 du 10 juillet 1991 précitée en a encadré le régime. Décidées par un magistrat indépendant, le juge d'instruction lorsqu'une information judiciaire est ouverte ou le juge des libertés et de la détention dans le cadre d'une enquête préliminaire [(2)], ces interceptions ne peuvent être ordonnées qu'« *en matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement* » et

---

(1) CEDH, 24 avril 1990, Kruslin c. France, *n° 11801/85.*

(2) Articles 74-2 et 706-95 du code de procédure pénale.

« *lorsque les nécessités de l'information l'exigent* » [1]. Elles sont réalisées dans les conditions prévues par les articles 100 à 100-7 du code de procédure pénale. Les correspondances avec un avocat relevant de l'exercice des droits de la défense et celles avec un journaliste permettant d'identifier une source ne peuvent être retranscrites. Ces interceptions, placées sous le contrôle étroit de l'autorité judiciaire, « *gardienne de la liberté individuelle* » aux termes de l'article 66 de la Constitution, sont donc étroitement encadrées.

L'accès aux métadonnées est également possible à des fins de police judiciaire, sur autorisation préalable du juge d'instruction dans le cadre d'une information judiciaire ou du juge des libertés et de la détention dans le cadre des enquêtes préliminaires et de flagrance. Mais, à la différence de la captation du contenu des conversations, cet accès est possible pour tout crime et délit, sans distinguer selon leur gravité [2].

En matière de géolocalisation judiciaire, qui permet de suivre en temps réel les déplacements d'une personne ou d'un objet par le suivi dynamique d'un terminal de communications électroniques ou l'implantation d'une balise sur un moyen de transport ou un objet, l'intervention du législateur en 2014, à la suite de deux arrêts rendus par la Cour de cassation, a permis d'encadrer précisément le recours à cette technique (voir l'encadré ci-après).

Les conditions de recours à la géolocalisation à des fins judiciaires

Avant 2014, la géolocalisation judiciaire était réalisée dans le cadre des dispositions générales du code de procédure pénale [1], sur décision du juge d'instruction ou du procureur de la République. La CEDH ayant estimé en 2010 qu'elle devait être prévue par une loi accessible au requérant et suffisamment précise et claire, assortie de garanties contre les abus de pouvoir et proportionnée au but légitime poursuivi, la Cour de cassation, par deux arrêts du 22 octobre 2013, a jugé que si elle était possible sur décision du juge d'instruction intervenant dans le cadre d'une information judiciaire, sur la base de l'article 81 du code de procédure pénale, elle ne pouvait être exécutée, dans le cadre d'enquêtes préliminaires ou de flagrance, que « *sous le contrôle d'un juge* » [2] indépendant au sens de la CESDH, ce qui excluait qu'elle fût ordonnée par le procureur de la République.

La loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation a tiré les conséquences de ces deux arrêts en définissant :

– les infractions pour lesquelles la géolocalisation est possible : infractions punies d'au moins cinq ans d'emprisonnement pour les délits d'atteinte aux biens, de trois ans pour les délits d'atteinte aux personnes, de recel de crime ou d'évasion, et de cinq ans pour les délits douaniers ;

– les conditions de son contrôle par le juge d'instruction et le juge des libertés et de la détention : si le parquet peut autoriser la géolocalisation pour une durée de quinze jours, dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou de l'une des procédures prévues aux articles 74 à 74-2 du code de procédure pénale, à l'issue de ce délai, l'opération doit être autorisée par le juge des libertés et de la détention, sur demande du procureur de la République, pour une durée maximale d'un mois renouvelable. Dans le cadre

(1) Premier alinéa de l'article 100 du même code.

(2) Articles 60-2, 77-1-2 et 99-4 du même code.

d'une instruction ou d'une information pour recherche des causes de la mort ou de la disparition, la géolocalisation est autorisée par le juge d'instruction, pour une durée maximale de quatre mois renouvelable. En cas d'urgence, un officier de police judiciaire peut recourir à une géolocalisation, sous réserve de l'autorisation *a posteriori* du procureur de la République obtenue dans les vingt-quatre heures.

Les règles applicables à la géolocalisation varient selon le lieu où le dispositif est implanté :

– dans les lieux privés destinés ou utilisés à l'entrepôt de véhicules, fonds, valeurs, marchandises ou matériel, ou dans un véhicule situé sur la voie publique, la géolocalisation doit être autorisée par le procureur de la République ou le juge d'instruction sans respecter les heures légales, le consentement et le droit à l'information de l'occupant des lieux ;

– dans les autres lieux privés (locaux professionnels, administrations, entreprises, etc.), la géolocalisation n'est possible que dans le cadre d'une enquête ou d'une instruction relative à un crime ou délit puni d'au moins cinq ans d'emprisonnement ou dans le cadre d'une procédure de recherche des causes de la mort ou d'une personne en fuite. S'il s'agit d'un lieu d'habitation, en cas d'enquête préliminaire, la géolocalisation doit être autorisée par le juge des libertés et de la détention saisi par le procureur de la République ; en cas d'information judiciaire, le juge d'instruction peut l'autoriser seul sauf si elle intervient en dehors des heures légales, auquel cas l'autorisation du juge des libertés et de la détention est nécessaire.

Dans tous les cas, la géolocalisation est interdite dans les locaux professionnels et le domicile des avocats et des journalistes, dans les locaux et véhicules d'une entreprise de presse et dans les cabinets des médecins, notaires et huissiers et ne peut pas concerner les parlementaires et les magistrats.

En matière de délinquance et de criminalité organisées, le juge des libertés et de la détention, saisi par le juge d'instruction, peut ordonner de ne pas joindre au dossier de la procédure certains éléments afin de protéger la vie d'un informateur, si leur connaissance met gravement en danger la vie ou l'intégrité physique d'une personne et à condition qu'elles ne soient ni utiles à la manifestation de la vérité, ni indispensables à l'exercice des droits de la défense.

(1) Articles 41, 60-2 et 77-1-1 du code de procédure pénale pour les enquêtes préliminaires ou en flagrance dirigées par le procureur de la République et article 81 du même code pour l'information judiciaire conduite par le juge d'instruction.

(2) Cass. crim., 22 octobre 2013, n°s 13-81.245 et 13-81.249.

Au-delà de l'interception des communications téléphoniques ou des métadonnées et de la géolocalisation, d'autres techniques d'investigation judiciaire sont nées avec les dernières évolutions technologiques ou se sont adaptées à l'ère numérique. C'est ainsi que le législateur a souhaité améliorer les moyens d'enquête des services de police et de justice afin de les adapter à la lutte contre la cyberdélinquance et la cybercriminalité.

Face au développement du stockage à distance (*cloud computing*) et au recours accru à des terminaux mobiles (tablettes, *smartphones*), il a autorisé la perquisition de données stockées à distance ou sur des terminaux mobiles à partir d'un système informatique implanté dans les services de police ou les unités de gendarmerie [(1)].

(1) Article 57-1 du code de procédure pénale.

Par ailleurs, pour tenir compte du développement des moyens de cryptologie destinés à renforcer la confidentialité des données, il a reconnu aux officiers de police judiciaire la faculté – aujourd'hui réservée à la seule autorité judiciaire – de requérir, sur autorisation du procureur de la République ou du juge d'instruction, toute personne qualifiée pour mettre au clair et décrypter les données [(1)].

Il a également peu à peu étendu le champ d'application de l'enquête sous pseudonyme (« cyberpatrouille » ou « cyberinfiltration ») à la constatation de plusieurs infractions commises par un moyen de communication électronique : les infractions de traite des êtres humains, proxénétisme, prostitution de mineurs ou de personnes vulnérables et mise en péril de mineurs [(2)], les infractions commises à l'occasion de paris ou de jeux d'argent ou de hasard en ligne [(3)], certaines infractions en matière sanitaire [(4)] et, tout récemment, les infractions relevant de la criminalité et de la délinquance organisées commises par un moyen de communication électronique [(5)].

Sans qu'il présente un caractère exhaustif, ce rapide panorama des nouvelles techniques d'enquête et d'investigation montre l'adaptation progressive des moyens de la police et de la justice aux dernières évolutions de la délinquance et de la criminalité. Destinées à permettre à l'État de remplir parfaitement son rôle en matière de sécurité, elles peuvent toutefois avoir de lourdes conséquences sur le droit au respect de la vie privée et à la protection des données des personnes qui en sont l'objet. Tel peut être le cas lorsque ladite technique est insuffisamment encadrée juridiquement ou est susceptible, par des effets collatéraux, de violer les droits fondamentaux de personnes qui, bien que liées à celle faisant l'objet de la mesure, ne sont pas impliquées dans l'infraction poursuivie.

2. Définir un régime juridique global, cohérent et protecteur des libertés fondamentales pour les activités de renseignement

En avril 2015, l'Assemblée nationale a examiné le projet de loi relatif au renseignement visant à actualiser les textes régissant les activités de renseignement dans un contexte marqué par les révélations de M. Edward Snowden sur la surveillance en ligne massive et généralisée des individus ainsi que par des menaces terroristes dont l'extrême gravité a été confirmée par les événements du mois de janvier 2015.

Le texte définitivement adopté fait d'incontestables progrès dans l'encadrement de l'utilisation des moyens à la disposition des services de renseignement. Il pose les principes et finalités de la politique publique de

---

(1) Articles 230-1 à 230-5 du même code.

(2) Articles 706-35-1 et 706-47-3 du même code.

(3) Article 59 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne.

(4) Article 706-2-2 du même code.

(5) Article 706-87-1 du même code.

renseignement, fixe la procédure d'autorisation des techniques de recueil du renseignement, définit la composition, les missions et les prérogatives de l'autorité administrative indépendante qui sera chargée de contrôler la mise en œuvre de ces techniques, introduit un recours juridictionnel permettant de contester cette mise en œuvre et encadre les conditions d'utilisation de chaque technique.

La Commission prend acte de la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015 qui a déclaré conformes à la Constitution la plupart des dispositions contenues dans ce texte. Elle **réitère** toutefois **les recommandations qu'elle a formulées au moment de l'examen par l'Assemblée nationale du projet de loi qui comporte selon elle des dispositions contestables et dangereuses pour les droits et libertés fondamentaux des individus, risquant, par des effets de brèche, de permettre le passage d'une surveillance ciblée à une surveillance généralisée** (1). Elle ne reviendra pas ici sur chacune de ses dispositions, notamment :

– la **définition imprécise des finalités de la surveillance administrative** ;

– l'**élargissement significatif du champ des interceptions de sécurité et du recueil administratif des données techniques de connexion et l'allongement de la durée de conservation des données ainsi collectées** ;

– l'**extension des moyens des services de renseignement à de nouvelles techniques** : dispositifs mobiles de proximité de captation directe de métadonnées, voire du contenu des communications (*IMSI-catchers*) ; recueil en temps réel, sur les réseaux des opérateurs de communications électroniques, des données de connexion de « *personnes préalablement identifiées comme présentant une menace* » (sonde) ; recours à des appareils de captation, de transmission et d'enregistrement de sons, d'images et de données informatiques ; introduction dans un véhicule, un lieu privé ou un système automatisé de traitement de données aux fins de poser, mettre en œuvre ou retirer de tels appareils ;

– l'**encadrement trop limité des conditions de la surveillance des communications émises ou reçues à l'étranger** : dans sa décision précitée, le Conseil constitutionnel a d'ailleurs considéré qu'« *en ne définissant dans la loi ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés (…), ni celles du contrôle par la commission nationale de contrôle des techniques de renseignement des autorisations délivrées (…) et de leurs conditions de mise en œuvre, le législateur n'a pas déterminé les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » (2) ;

– la **potentielle faiblesse des moyens et prérogatives accordés à la nouvelle Commission nationale de contrôle des techniques de renseignement** (CNCTR) ;

---

(1) Voir la recommandation du 1er avril 2015 sur le projet de loi relatif au renseignement.

(2) Décision n° 2015-713 DC du 23 juillet 2015, Loi relative au renseignement, considérants 76 à 79.

– l'**insuffisante incrimination des activités de surveillance illégales**.

Elle souhaite renouveler sa mise en garde sur les dangers soulevés par le **nouvel article L. 851-3 du code de la sécurité intérieure** qui autorise l'exploitation, par les opérateurs de communications électroniques et les fournisseurs de services, des informations et documents traités par leurs réseaux afin de détecter des connexions susceptibles de révéler une menace terroriste (détection de « signaux faibles » par la pose de « boîtes noires » chez les opérateurs).

Malgré les précisions apportées à son dispositif et les garanties supplémentaires entourant sa mise en œuvre, la Commission estime que **cet article ouvre la voie à une collecte massive et à un traitement généralisé de données personnelles et que ce type de technologies** – dont l'inefficacité a été prouvée dans les pays qui l'ont utilisée – **n'est, en l'état des informations disponibles, pas susceptible d'un encadrement strict**.

Recommandation n° 69

Interdire le recours à des dispositifs algorithmiques de traitements de données transitant par les réseaux numériques aux fins de détection de « signaux faibles » ou de menaces, quelle que soit la finalité poursuivie.

En outre, la Commission se félicite que le Conseil constitutionnel ait déclaré contraires à la Constitution les dispositions du nouvel article L. 821-6 du même code qui instituait une procédure dérogatoire d'installation, d'utilisation et d'exploitation des appareils ou dispositifs techniques de localisation en temps réel d'une personne, d'un véhicule ou d'un objet, d'identification d'un équipement terminal ou du numéro d'abonnement ainsi que de localisation de cet équipement ou d'interception des correspondances émises ou reçues par cet équipement « *en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement* ». Cette procédure dite d'urgence opérationnelle, encore plus dérogatoire que celle, exceptionnelle, de l'urgence absolue, aurait permis de déroger à la délivrance préalable d'une autorisation par le Premier ministre – qui n'aurait du reste même pas été préalablement informé de la mise en œuvre d'une technique de renseignement – et de l'avis de la CNCTR, ce qui constituait, ainsi que l'a relevé le Conseil constitutionnel, « *une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* » (1).

Au-delà de ces considérations, la Commission a souhaité se concentrer sur le cadre juridique général dans lequel les activités de surveillance administrative devraient s'inscrire à l'ère numérique. Pour cela, elle recommande de **définir un régime juridique global, cohérent et protecteur des libertés fondamentales pour les activités de renseignement**, ménageant un juste équilibre entre les nécessités constitutionnelles de préservation de l'ordre public – à laquelle les

(1) Décision n° 2015-713 DC du 23 juillet 2015 précitée, considérants 27 à 30.

services de renseignement participent – et les droits de chacun au respect de sa vie privée, de sa correspondance, de son domicile et de ses données personnelles.

D'une part, ce régime doit respecter le principe du secret des correspondances et des communications électroniques, qui ne peuvent être surveillées que « *dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* » (1), sous le contrôle de l'autorité judiciaire ou d'un mécanisme présentant des garanties suffisantes.

D'autre part, il doit être conforme à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 et à l'article 8 de la CESDH aux termes duquel il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée et familiale, du domicile et de la correspondance que pour autant qu'elle est prévue par une loi accessible et prévisible et qu'elle est nécessaire, dans une société démocratique, à la poursuite d'un but légitime. La CEDH insiste sur le caractère prévisible et accessible de la loi, qui « *doit user de termes assez clairs pour indiquer aux individus de manière suffisante en quelles circonstances et sous quelles conditions elle habilite les autorités publiques à prendre des mesures de surveillance secrète* ». Ainsi, la Cour estime que « *les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance. Partant, elles doivent se fonder sur une "loi" d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner* » (2).

En pratique, ce régime doit **embrasser l'ensemble des techniques et moyens à la disposition des services de renseignement**. En contrepartie de cette clarification, la Commission recommande de mettre un terme aux éventuelles pratiques illégales des services en renforçant significativement les **sanctions pénales des infractions résultant d'actions contraires à la loi**.

Recommandation n° 70

Encadrer par la loi le recours à l'ensemble des techniques et moyens susceptibles d'être à la disposition des services de renseignement pour remplir leurs missions et mettre un terme aux éventuelles pratiques illégales en sanctionnant plus durement les infractions à la législation.

Ce régime doit également **prévoir, pour chaque technique de renseignement, des garanties appropriées et équivalentes, quel que soit leur prétendu degré d'intrusion dans la vie privée**. Comme elle l'a déjà dit, la Commission estime qu'à l'ère numérique, il est aussi intrusif de connaître le contenu de conversations privées que d'accéder à des données renseignant sur la connexion d'individus à tel ou tel service de communications.

---

(1) CEDH, 6 septembre 1978, Klass et autres c. Allemagne.

(2) CEDH, 24 avril 1990, Kruslin c. France, *n° 11801/85.*

Recommandation n° 71

Soumettre chaque technique de renseignement à des garanties appropriées et équivalentes, quel que soit leur prétendu degré d'intrusion dans la vie privée.

Afin d'être véritablement **protecteur des libertés fondamentales**, ce régime doit satisfaire à au moins quatre exigences :

– la **définition précise des conditions et motifs des atteintes portées aux libertés individuelles**, allant au-delà d'un simple renvoi à des notions trop générales comme la défense des « *intérêts fondamentaux de la Nation* » ;

– l'**affirmation des principes de proportionnalité et de subsidiarité**, limitant au strict nécessaire ces atteintes et exigeant qu'elles ne soient envisagées que si seulement aucun autre moyen légal ne peut parvenir au même résultat ;

– l'**encadrement de la surveillance des communications à l'étranger**, aujourd'hui marquée par une réelle opacité, afin de s'assurer que les correspondances et métadonnées qui impliqueraient des citoyens français seront soumises au régime juridique commun ;

– l'**instauration de voies de recours effectives** permettant à tout citoyen de contester certaines pratiques et de faire valoir ses droits.

Recommandation n° 72

Accorder aux citoyens des garanties fondamentales face aux activités de surveillance administrative par la définition précise des conditions et motifs des atteintes susceptibles d'être portées aux droits à la vie privée et à la protection des données personnelles, la réaffirmation de leur proportionnalité et subsidiarité, l'encadrement de la surveillance des communications à l'étranger et l'instauration de voies de recours effectives pour contester certaines pratiques.

Par ailleurs, la Commission estime indispensable de **soumettre ces activités au contrôle permanent d'une autorité indépendante et impartiale, disposant de moyens humains, matériels, techniques et financiers suffisants**. Cette autorité devrait reprendre les compétences aujourd'hui exercées par la CNCIS sous une forme et un périmètre d'action élargis. Pour la Commission, l'indépendance institutionnelle de cette autorité devrait être garantie par la loi qui devrait préciser qu'elle ne peut recevoir d'instruction d'aucune autre autorité, qu'elle est soumise au seul contrôle de la Cour des comptes et que la qualité de membre de cette institution est incompatible avec certaines fonctions.

Recommandation n° 73

Instaurer un contrôle externe permanent de la mise en œuvre des techniques de renseignement par la création d'une autorité administrative indépendante et impartiale, dotée des moyens humains, matériels, techniques et financiers suffisants.

Son contrôle devrait s'exercer sur l'ensemble des services de renseignement et l'intégralité des mesures et techniques qu'ils emploient, en amont de leur mise en œuvre sous la forme d'un avis préalable, durant leur application et en aval, sous la forme de contrôles sur pièces et sur place. Outre un pouvoir de recommandation, cette autorité devrait pouvoir transmettre au juge les cas dans lesquels elle estime que le pouvoir exécutif a méconnu les garanties accordées par la loi au citoyen.

En complément de ce contrôle externe doivent continuer de s'appliquer le contrôle interne et interministériel des services par l'inspection du renseignement mise en place en 2014 (1) – dont il convient de renforcer les moyens et les prérogatives d'investigation afin d'en faire un contrôle interne méthodique et incontestable – et le contrôle politique de l'action du Gouvernement par la délégation parlementaire au renseignement créée en 2007 (2).

Recommandation n° 74

Confier à cette autorité des compétences élargies à l'ensemble des services de renseignement et à l'intégralité des mesures qu'ils sont susceptibles de prendre, en lui donnant des prérogatives de contrôle *a priori*, en cours d'opération et *a posteriori* ainsi qu'un pouvoir de recommandation et en lui permettant de saisir un juge en cas de méconnaissance des obligations légales par le pouvoir exécutif.

À l'instar de ce qu'elle a déjà proposé pour faire connaître et cesser les activités illégales des acteurs privés en matière de traitements de données personnelles (3), la Commission souhaite la **création d'un droit de signalement des activités illégales au profit des agents des services de renseignement qui souhaiteraient révéler des manquements à la législation ou des pratiques contestables**. Ainsi que l'a souligné M. William Bourdon lors de son audition le 25 septembre 2014, certaines de ces pratiques révèlent des manquements à la morale, à l'éthique ou à l'intérêt général parfois plus graves que des délits, qui ne sont pas couverts par les dispositions de l'article 40 du code de procédure pénale

---

(1) Par le décret n° 2014-833 du 24 juillet 2014 relatif à l'inspection des services de renseignement.

(2) En application de l'article 6 nonies *de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.*

(3) Voir supra, *le* c *du 3 du B du présent III.*

ou le droit d'alerte général prévu par le code du travail et le statut général des fonctionnaires [(1)].

Ce droit de signalement des activités illégales pourrait d'abord s'exercer au sein du service concerné – par exemple auprès de l'inspection du renseignement – puis devant l'autorité administrative indépendante chargée de contrôler la mise en œuvre des techniques de renseignement. En toute hypothèse, le lanceur d'alerte devrait être en mesure d'agir sans se mettre en danger.

À cet égard, la Commission salue l'introduction par la loi relative au renseignement d'un nouvel article L. 861-3 dans le code de la sécurité intérieure. Cet article prévoit que « [t]*out agent d'un service (…)* [de renseignement] *qui a connaissance, dans l'exercice de ses fonctions, de faits susceptibles de constituer une violation manifeste (…)* [du cadre légal des activités de renseignement] *peut porter ces faits à la connaissance de la seule Commission nationale de contrôle des techniques de renseignement qui peut alors saisir le Conseil d'État (…) et en informer le Premier ministre. (…) Lorsque la commission estime que l'illégalité constatée est susceptible de constituer une infraction, elle saisit le procureur de la République dans le respect du secret de la défense nationale et transmet l'ensemble des éléments portés à sa connaissance à la Commission consultative du secret de la défense nationale afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République* ». L'agent fait également l'objet d'une protection spécifique contre toute mesure défavorable qui pourrait être prise à son encontre en raison de ce signalement. Néanmoins, la Commission regrette vivement qu'ait été supprimé, juste avant l'adoption définitive du texte, un important alinéa de cet article, précisant que « *l'agent (…) peut, dans le seul cadre de la relation ou du témoignage réalisé devant la commission, faire état d'éléments ou d'informations protégés au titre du secret de la défense nationale ou susceptibles de porter atteinte à la sécurité des personnels ou des missions des services mentionnés à l'alinéa précédent* ».

Recommandation n° 75

Créer un droit de signalement devant l'autorité administrative indépendante chargée de contrôler la mise en œuvre des techniques de renseignement permettant aux agents impliqués dans ces activités de mettre au jour des pratiques illégales.

Enfin, la Commission appelle tout particulièrement l'attention sur la **question de la conservation des données techniques de connexion à la suite de l'invalidation par la CJUE en avril 2014 de la directive européenne qui en règle partiellement les dispositions** [(2)].

---

(1) Voir supra, *le même* c.

(2) CJUE, 8 avril 2014, Digital Rights Ireland et Seitlinger, *n^os^ C-293/12 et C-594/12.*

Jusqu'alors, la 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 permettait aux États d'adopter des mesures prévoyant la conservation des métadonnées pendant une durée comprise entre six mois et deux ans. En France, aux termes de l'article L. 34-1 du code des postes et des communications électroniques, les opérateurs de communications électroniques conservent les données de connexion de leurs clients pendant une durée maximale d'un an.

En invalidant la directive 2006/24/CE du 15 mars 2006 précitée, la CJUE a jugé que les règles communautaires régissant la conservation des métadonnées (champ des données concernées, durée) constituaient une ingérence particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel protégés par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Elle a considéré que si elle était justifiée par des buts d'intérêt général, la lutte contre le terrorisme et la criminalité organisée, cette ingérence était disproportionnée en couvrant « *de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre les infractions graves* » (1), en ne prévoyant « *aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure* » (2) et en fixant une durée de conservation sans tenir compte de l'utilité de la conservation par rapport aux objectifs poursuivis.

La Commission invite les législateurs national et européen à **tirer les conséquences de l'invalidation de cette directive,** même si de nombreuses incertitudes entourent aujourd'hui l'interprétation exacte qu'il convient de donner à l'arrêt de la CJUE et l'applicabilité des dispositions de la Charte des droits fondamentaux de l'Union européenne aux législations nationales prises en la matière (3).

Si la CJUE ne s'est pas prononcée sur des durées précises de conservation des métadonnées ni sur la durée française établie à un an, une interprétation stricte de sa décision, selon laquelle elle aurait condamné le caractère général, indiscriminé et uniformément durable de la conservation des métadonnées, devrait, selon la Commission, conduire le législateur à revoir le droit existant et à mieux proportionner la durée de cette conservation. Cela vaut pour la conservation des données techniques de connexion auxquelles l'autorité administrative souhaite accéder mais également pour l'accès aux métadonnées à des fins de police

---

(1) Op. cit., *§ 57.*

(2) Op. cit., *§ 60.*

(3) Pour plus de précisions sur cette question précise, voir Conseil d'État, op. cit., *pp. 199-201.*

judiciaire, qui pourrait être réservé à la poursuite des infractions d'une particulière gravité et non, comme c'est le cas aujourd'hui, pour tout crime ou délit.

Recommandation n° 76

Tirer les conséquences juridiques adéquates de l'arrêt de la CJUE *Digital Rights Ireland et Seitlinger* du 8 avril 2014 en limitant la durée de conservation des données techniques de connexion au strict nécessaire ainsi que l'étendue de l'accès accordé à ces données aux autorités publiques.

3. Mieux encadrer les nouveaux moyens donnés par le numérique aux services de police et de justice

S'agissant des moyens numériques spéciaux d'investigation, la Commission renvoie aux recommandations qu'elle a déjà formulées au moment de l'examen, par l'Assemblée nationale, de la loi renforçant les dispositions relatives à la lutte contre le terrorisme [(1)] qui a autorisé le recours à plusieurs techniques d'enquête potentiellement intrusives aux fins de prévenir les actions terroristes et de combattre la délinquance et la criminalité organisées.

Elle ne conteste pas que ces moyens soulèvent moins de problèmes pour la protection des libertés fondamentales dans la mesure où ils sont mis en œuvre sous le contrôle de l'autorité judiciaire et pour la poursuite de certaines infractions limitativement énumérées. Elle souhaite toutefois qu'à l'avenir, le législateur encadre encore davantage les nouveaux moyens d'enquête que le numérique donne aux services de police et de justice.

Si certaines dispositions relatives à l'accès aux données informatiques, à leurs saisies et à leur exploitation sont devenues obsolètes et inadaptées à la lutte contre la cybercriminalité, la Commission considère que leur actualisation doit se faire **en conformité avec les exigences de subsidiarité et de proportionnalité**.

À cette fin, elle recommande d'**accorder toutes les garanties nécessaires à la protection de la personne concernée par ces mesures** et de **conditionner systématiquement leur mise en œuvre à l'autorisation préalable d'un magistrat indépendant**, autorisation qui doit être **limitée dans le temps**. De même, le recours à des personnes qualifiées et à des experts pour déchiffrer et exploiter les données informatiques saisies doit faire l'objet de l'autorisation préalable d'un juge et être strictement encadré, afin de s'assurer de l'indépendance et de la qualification des personnes qui interviennent dans la procédure judiciaire et garantir qu'il ne sera pas porté aux droits au respect de la vie privée et à la protection des données personnelles une atteinte disproportionnée et injustifiée. Elle souhaite également que cet encadrement comporte des **règles particulières**

---

(1) Voir la recommandation du 29 septembre 2014 sur plusieurs articles du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme.

destinées à renforcer les garanties applicables à certaines personnes traditionnellement protégées par le code de procédure pénale, à l'instar des avocats, journalistes, médecins, notaires, huissiers, magistrats ou parlementaires.

Par ailleurs, la Commission invite le législateur à **délimiter strictement le champ des infractions pour lesquelles de telles mesures peuvent être mises en œuvre en les cantonnant à la poursuite des infractions criminelles et délictuelles les plus graves ou les plus organisées**. Tel devrait notamment être le cas du recours à l'enquête sous pseudonyme ou à la captation à distance de certaines informations à des fins judiciaires. Elle observe à cet égard avec inquiétude l'extension progressive du champ de la cyberinfiltration à un nombre croissant d'infractions, d'une gravité variable [(1)].

Recommandation n° 77

Encadrer strictement l'utilisation par les services de police et de justice des techniques spéciales d'investigation susceptibles de porter atteinte aux droits au respect de la vie privée et à la protection des données personnelles :

– les soumettre à l'autorisation préalable d'un magistrat judiciaire indépendant et limitée dans le temps ;

– prévoir des garanties renforcées lorsqu'elles s'appliquent à certaines professions ou fonctions traditionnellement protégées par le code de procédure pénale ;

– les cantonner à la poursuite des infractions délictuelles et criminelles les plus graves.

Enfin, comme pour les activités de surveillance administrative, elle préconise d'**écarter, au présent et à l'avenir, toute exploitation systématique de données personnelles rendues disponibles sur les réseaux et leur croisement avec d'autres informations ou le recours massif et indiscriminé à des technologies intrusives qui permettraient de prédire la probabilité qu'un fait délictueux ou criminel se produise** à tel endroit et à tel moment.

Pour futuriste qu'elle soit en France, cette perspective est d'ores et déjà une réalité dans certains pays qui se sont dotés, en matière de sécurité urbaine, de techniques de **police prédictive** [(2)], comme aux États-Unis avec le programme *Blue CRUSH* [(3)] mis en place par la ville de Memphis, la *predictive policing* mise en place dès 2008 par la police de Los Angeles, ou au Royaume-Uni avec le *Total Technology Strategy* 2014-2017 de la *metropolitan police* de Londres par exemple.

---

(1) Voir supra, *le* b *du 1 du présent C.*

(2) Voir Élisabeth Grosdhomme Lulin, op. cit., *pp. 27-28.*

(3) Crime Reduction Using Statistical History.

Dans ce contexte, le législateur doit veiller à examiner, dans leur ensemble et au regard de leur impact conjugué, les moyens et technologies à la disposition des services de police et de justice (fichiers de sécurité, vidéosurveillance et vidéoprotection, nouveaux moyens d'investigation numérique, etc.), afin de prévenir l'apparition de programmes de surveillance judiciaire de masse et disproportionnés par rapport aux objectifs légitimes de prévention de la délinquance et de répression des infractions.

Recommandation n° 78

Comme en matière de renseignement, écarter la mise en œuvre de programmes conduisant à l'exploitation et au croisement systématiques et à grande échelle des données disponibles sur les réseaux ou recueillies par des technologies de surveillance.

*

* *

En définitive, s'il n'est évidemment pas un « monde à part », échappant aux nécessités liées à la préservation de l'ordre public ou aux règles induites par l'innovation technologique et la concurrence entre acteurs privés, le monde numérique ne doit pas non plus être l'occasion ou le moyen d'introduire des régressions en matière de libertés fondamentales, notamment quant aux droits au respect de la vie privée et à la protection des données personnelles.

IV. DÉFINIR DE NOUVELLES GARANTIES INDISPENSABLES À L'EXERCICE DES LIBERTÉS À L'ÈRE NUMÉRIQUE

Le numérique révolutionne les conditions d'exercice de plusieurs libertés fondamentales traditionnelles (liberté d'expression et de communication, droit à l'information, liberté d'entreprendre et d'innovation, liberté d'association, droits culturels…). Il suscite également la reconnaissance de nouveaux principes et de nouvelles règles spécifiques indispensables à l'exercice de ces libertés dans l'univers numérique. Ces principes forment dès lors un ensemble de droits que l'on pourrait qualifier de « natifs du numérique ».

En premier lieu, compte tenu du rôle essentiel joué par internet dans l'exercice des droits et libertés, l'accès à internet tend à être reconnu, en France comme dans d'autres pays et au plan international, comme un droit à part entière. La Commission propose d'aller plus loin dans sa consécration (**A**).

En deuxième lieu, si la neutralité du réseau, consubstantielle à son architecture, est ce qui permet à tout individu, toute entreprise ou toute association de bénéficier d'un égal accès à tous les internautes, elle est, comme le droit d'accès, une garantie essentielle de la liberté d'expression, du droit à l'information, de la liberté d'entreprendre et de la liberté d'association. Face au développement de pratiques des opérateurs de communications électroniques tendant à remettre en cause cette neutralité, il convient d'aller plus loin dans la reconnaissance de ce principe dans le droit positif (**B**).

Enfin, au-delà des réseaux physiques, d'autres intermédiaires privés, en particulier les grandes « plateformes » numériques, jouent un rôle central dans l'accès des utilisateurs finaux aux informations, contenus, services et applications proposés. C'est pourquoi la protection des libertés à l'âge numérique implique de mieux appréhender les problèmes spécifiques soulevés par les activités de ces acteurs, à travers l'adaptation du droit commun, qui pourrait être complétée par la mise en place d'une régulation spécifique (**C**).

A. LE DROIT D'ACCÈS À INTERNET : UN DROIT À RENFORCER

Pour la Commission, il s'agit ni plus ni moins que de reconnaître le droit d'accès de chaque citoyen aux infrastructures essentielles de la modernité dans la mesure où l'accès aux réseaux conditionne l'égalité réelle d'accès à de nombreux droits.

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

démocratique et l'expression des idées et des opinions » [1], **l'exercice de la liberté de communication et d'expression**, protégée par l'article 11 de la Déclaration des droits de l'homme et du citoyen, **implique la liberté d'accéder à internet**. Le Conseil était alors saisi d'une loi qui prévoyait de confier à la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI), autorité administrative indépendante, le pouvoir de prononcer une sanction administrative de suspension de l'accès à internet à l'encontre d'une personne n'ayant pas veillé à ce que cet accès ne soit pas utilisé pour diffuser ou recevoir des contenus en méconnaissance des droits des auteurs. Le Conseil a censuré cette disposition en indiquant que seule l'autorité judiciaire était habilitée à prononcer une telle peine.

La question de savoir si la liberté d'accéder à internet, ainsi reconnue par le Conseil, constitue un nouveau droit fondamental n'est cependant pas tranchée. Le droit d'accès à internet a fait l'objet d'une reconnaissance dont la portée demeure limitée (**1**) de sorte que le débat se prolonge aujourd'hui sur l'opportunité de le consacrer plus explicitement (**2**).

1. Le droit d'accès à internet, une reconnaissance dont la portée demeure limitée

En France, depuis la décision « Hadopi » du 10 juin 2009, certains observateurs estiment que l'accès à internet constitue un droit fondamental. Ainsi, pour Mme Laure Marino, le Conseil constitutionnel aurait-il élevé la liberté d'accès à internet au rang de nouveau droit fondamental [2] : « *pour ce faire, le Conseil constitutionnel utilise la méthode d'annexion qu'il affectionne. Il décide que la liberté de communication et d'expression "implique" désormais la liberté d'**accès** à **internet**. Comme dans un jeu de poupées russes, cela signifie qu'elle l'intègre et l'enveloppe ou, mieux encore, qu'elle l'annexe. On peut se réjouir de cette création d'un nouveau droit-liberté : le droit d'accès à internet. L'accès à internet devient ainsi, en lui-même, un droit-liberté, en empruntant par capillarité la nature de son tuteur, la liberté d'expression. Ainsi inventé par le Conseil, le droit d'être connecté à internet est donc un **droit** constitutionnel dérivé de l'article 11 de la Déclaration des **droits** de l'homme et du citoyen de 1789* ». De même, dans son étude annuelle 2014, le Conseil d'État qualifie le droit d'accès de nouveau droit fondamental [3].

La décision du Conseil constitutionnel a été prolongée par d'autres décisions prises au niveau européen qui plaident en faveur d'une telle reconnaissance au plan européen.

---

(1) Décision n° 2009-580 DC du 10 juin 2009, Loi favorisant la diffusion et la protection de la création sur internet, *considérant 12.*

(2) Laure Marino, « Le droit d'accès à internet, nouveau droit fondamental », Dalloz 2009, 3 septembre 2009, p. 2045.

(3) Conseil d'État, op. cit., *p. 90.*

À titre d'exemple, dès 2009, et en plein débat sur la loi « Hadopi » que devait adopter la France quelques semaines plus tard, le Parlement européen s'est symboliquement opposé, par une recommandation [(1)], à la riposte graduée et à l'hypothèse de la coupure de l'accès internet. Les députés européens se sont prononcés favorablement par 481 voix contre 25 (et 21 abstentions) en estimant qu'un tel accès ne devait pas être utilisé comme une sanction par les Gouvernements. Dans le même esprit, la directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 [(2)], composante du troisième paquet télécoms dispose que « *les mesures prises par les États membres concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de communications électroniques respectent les libertés et droits fondamentaux des personnes physiques tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et les principes généraux du droit communautaire* ». La directive impose par conséquent le respect de la présomption d'innocence et la mise en place d'une procédure « *préalable, équitable et impartiale* » avant toute restriction de l'accès.

D'autres observateurs se montrent plus prudents et soulignent que l'accès à internet doit être considéré comme un facilitateur de droits et non comme un droit en lui-même. Début 2012, dans un article intitulé « *L'accès à internet n'est pas un droit de l'Homme* » publié par le *New York Times*, M. Vinton Cerf, inventeur du protocole TCP/IP, considéré comme l'un des pères d'internet, rappelait ainsi qu'en dépit du rôle central joué par internet pour l'exercice des droits (rôle mis particulièrement en lumière au cours des révolutions arabes), « *la technologie est un facilitateur de droits, pas un droit en lui-même* ». Pour M. Vinton Cerf, faire entrer une technologie dans cette « magnifique catégorie » que sont les droits de l'Homme revient à « *donner de la valeur au mauvais objet* ».

Dans le même esprit, pour M. Michaël Bardin, docteur en droit public, « *La désormais très fameuse décision n° 2009-580 DC du Conseil constitutionnel (…) a une portée de la plus grande importance mais* ***reste très encadrée quant à la reconnaissance d'un droit d'accès à internet****. En effet, les promoteurs de cette reconnaissance ont rapidement conclu que le Conseil constitutionnel venait de reconnaître cet accès comme un droit fondamental. Pourtant, il apparaît nécessaire de* ***relativiser cette reconnaissance*** *et d'****en apprécier toutes les limites****. (…) Les juges, par cette décision, confirment bien qu'il est nécessaire de reconnaître l'importance contemporaine du droit d'accès à internet mais, pour autant, le droit d'accès à internet n'est ni «* un *droit* de l'Homme *» ni un « droit* fondamental *» en lui-même. Il n'est et n'existe que comme moyen de*

---

(1) Recommandation du Parlement européen du 26 mars 2009 à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur internet, n° 2008/2160 (INI).

(2) Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.

concrétisation de la liberté d'expression et de communication. En définitive, le droit d'accès à internet vient prendre sa juste place dans les moyens déjà connus et protégés que sont la presse, la radio ou encore la télévision » (1).

La Commission estime que le droit d'accès à internet est devenu, plus qu'un facilitateur de droits, « *un outil indispensable pour le respect de toute une catégorie de droits de l'Homme* » comme l'indiquait en mai 2011, un rapport des Nations unies (2). Le Conseil constitutionnel a reconnu le droit d'accès comme une condition d'exercice de la seule liberté d'expression et de communication. Or, comme le souligne M. Franck La Rue, rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, dans un rapport du 10 août 2011, « *l'accès à internet est indispensable non seulement à l'exercice du droit à la liberté d'expression mais aussi à celui d'autres droits, dont le droit à l'éducation, le droit de s'associer librement avec d'autres et le droit de réunion, le droit de participer pleinement à la vie sociale, culturelle et politique et le droit au développement économique et social* ». Comme l'indique le Conseil d'État dans son étude annuelle 2014, la liberté d'entreprendre, qui découle de l'article 4 de la Déclaration des droits de l'homme et du citoyen, implique le droit pour les entreprises de développer des activités à caractère numérique. « *La loi et la jurisprudence présentent aujourd'hui plusieurs garanties de ce que l'on pourrait qualifier de « droit à une existence numérique » de l'entreprise, qui implique différents attributs : droit à un nom de domaine, droit à fournir des services sur internet, droit d'utiliser certains instruments tels que la publicité, la cryptographie ou les contrats conclus par voie électronique* » (3). Il va sans dire que la liberté d'entreprendre et le droit à une existence numérique impliquent également le droit d'accéder à internet. L'accès à internet comporte donc indéniablement des enjeux qui dépassent largement ceux de l'accès à la presse, la radio ou la télévision.

Quoi qu'il en soit, la décision n° 2009-580 DC du Conseil constitutionnel ne reconnaît pour le citoyen qu'un droit à ne pas voir son accès à internet coupé sur décision d'une autorité administrative indépendante. La riposte graduée pouvant conduire à une peine de coupure d'accès est en revanche validée, à condition qu'elle soit prononcée par un juge.

Le débat se prolonge donc en France comme ailleurs sur l'étendue qu'il convient de donner à ce droit et en particulier sur l'existence d'un droit-créance qui s'accompagnerait d'**obligations positives des pouvoirs publics** afin de permettre l'accès de chacun à internet.

---

(1) Mickaël Bardin, « Le droit d'accès à internet : entre « choix de société » et protection des droits existants », Revue Lamy droit de l'immatériel, *2013, n° 91.*

(2) Haut-Commissariat aux droits de l'Homme, Rapport du 16 mai 2011, A/HRC/17/27.

(3) Conseil d'État, op. cit., *p. 104.*

2. Un droit à renforcer

Le rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, M. Franck La Rue, dans un rapport du 10 août 2011, estimait que « *bien que l'accès à internet ne soit* ***pas encore un droit de l'Homme en tant que tel***, (...) *les États ont pour* ***obligation positive*** *de promouvoir ou de faciliter l'exercice de la liberté d'expression et de fournir les moyens nécessaires à l'exercice de ce droit, notamment internet* » (1).

À la suite de la décision du Conseil constitutionnel, la professeure Laure Marino préconisait d'aller plus loin à travers la mise en place d'un « ***service public de l'accès à internet****, comme il existe un service public de l'éducation. Un service public français puis, soyons fous, un service public européen* ! » (2).

Certains pays sont allés plus loin dans la reconnaissance d'un droit-créance d'accès à internet. Depuis 2010, le législateur finlandais a fait du droit d'accès à internet, et même d'un accès à haut débit, un **droit opposable**. Les fournisseurs d'accès à internet (FAI) ont l'obligation de proposer à chaque citoyen finlandais une connexion minimale de 1 Mbit/s. La Finlande a modifié, dès 2009, sa loi sur le marché des communications pour que l'accès suffisant à l'internet devienne un « **service universel** », au même titre que le téléphone ou encore la poste. La législation finlandaise prévoit également que le **prix** de l'abonnement doit être « ***raisonnable*** » même si l'Autorité finlandaise de régulation des communications confirme que cet abonnement « *peut prendre en compte le coût induit par la production de ce service* » (3).

En Estonie, le mouvement s'est amorcé encore plus tôt. Dès 2000, à travers la loi sur les communications, le Parlement estonien a prévu la mise en place d'un « **service universel** », à savoir un « *ensemble de services* [garantissant] *que, dans une zone géographique déterminée par la licence accordée à un opérateur téléphonique, tous les clients qui souhaitent accéder aux réseaux publics de téléphonie puissent le faire à* ***un coût raisonnable et uniforme*** ». Ce service universel doit se concrétiser par « *un service internet universellement accessible à tous les abonnés, quelle que soit leur localisation géographique, à un prix uniforme* ». La même année, dans un autre texte, le Parlement estonien a entériné cette volonté de garantir l'accès à internet de l'ensemble de la population en prévoyant « *la possibilité d'un accès gratuit à l'information publique* via *internet dans les bibliothèques publiques* ».

Dans le même esprit, le **projet de déclaration des droits sur internet élaboré par la Commission d'étude sur les droits et devoirs sur internet de la chambre des députés italienne** tend à consacrer le droit pour toute personne « *d'accéder à internet dans des conditions d'égalité, suivant des modalités*

---

(1) Rapport du Rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 10 août 2011.

(2) Laure Marino, op. cit.

(3) Voir Mickaël Bardin, op. cit.

technologiquement adéquates et actualisées qui lèvent tout obstacle d'ordre économique et social ». La Commission italienne propose de consacrer le principe selon lequel *« la protection effective du droit d'accès* ***exige des interventions publiques adéquates pour surmonter toute forme de fracture numérique – culturelle, infrastructurelle, économique – en ce qui concerne notamment l'accessibilité de la part des personnes handicapées*** ».

Dans un rapport d'information de juin 2011, *Révolution numérique et droits de l'individu : pour un citoyen libre et informé*, MM. Patrick Bloche et Patrice Verchère estimaient également que le droit d'accès reconnu par le Conseil constitutionnel devait se prolonger par des mesures positives destinées à favoriser l'accès de chacun à internet : **lutte contre les différentes fractures numériques** ; mise en place d'une **tarification sociale de l'internet** ; **déploiement d'un réseau d'espaces numériques publics** (EPN) ; **protection des personnes en difficulté risquant de perdre leur connexion à internet** ; **mesures destinées à rendre internet plus accessible aux personnes handicapées** (1). De même, un rapport de juin 2013 du Conseil national du numérique consacré à l'inclusion numérique préconisait une gamme de mesures, notamment le développement de tarifs sociaux ciblés pour l'internet et le mobile ainsi que des espaces publics numériques (2). Cependant, la directive n° 2002/22/CE du 7 mars 2002, dite « directive service universel » (3), ne permet pas d'inclure la fourniture de tels tarifs sociaux couvrant l'accès à internet dans les obligations de service universel financées par la contribution des opérateurs ; ils peuvent donc seulement être aujourd'hui proposés de manière volontaire par les opérateurs.

La Commission souhaite que le droit d'accès à internet, qui conditionne l'exercice de plusieurs droits fondamentaux et qui exige des interventions publiques pour lutter contre toute forme de fracture numérique, fasse l'objet d'une consécration plus explicite au plan national et au plan européen et que l'accès à internet soit érigé au rang de service universel.

Recommandation n° 79

Reconnaître aux plans national et européen le droit d'accès à internet comme condition d'exercice de plusieurs droits fondamentaux. Préciser que la protection effective de ce droit exige des interventions publiques adéquates pour surmonter toute forme de fracture numérique – culturelle, infrastructurelle, économique – en ce qui concerne l'accessibilité.

Réformer la directive service universel du 7 mars 2002 afin de permettre la mise en place d'une tarification sociale de l'internet.

---

(1) Rapport d'information (n° 3560, XIIIe législature) de MM. Patrick Bloche et Patrice Verchère pour la mission d'information commune sur les droits de l'individu dans la révolution numérique, juin 2011, pp. 265-289.

(2) Conseil national du numérique, Citoyens d'une société numérique, *novembre 2013.*

(3) Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques.

Dans le même temps, la Commission est d'avis que l'effectivité du droit d'accès à l'internet doit être renforcée par l'instauration d'un **droit pour chacun d'accéder à la « littératie » numérique**, qui se définit comme l'« *aptitude à comprendre et à utiliser* [le numérique] *dans la vie courante, à la maison, au travail et dans la collectivité en vue d'atteindre des buts personnels et d'étendre ses compétences et capacités* » (1). Comme l'affirme l'Académie des sciences, il s'agit de « *donner à tous les citoyens les clés du monde du futur, qui sera encore bien plus numérique et donc informatisé que ne l'est le monde actuel, afin qu'ils le comprennent et puissent participer en conscience à ses choix et à son évolution plutôt que de le subir en se contentant de consommer ce qui est fait et décidé ailleurs* » (2).

Dans son rapport *Citoyens d'une société numérique*, le Conseil national du numérique faisait de cet accès un « *impératif moral et une nécessité économique* ». Ainsi, « *chaque personne passée par l'éducation nationale* [devrait] *y avoir acquis une littératie numérique. De même, chaque personne ayant suivi une formation professionnelle* [devrait] *y avoir acquis les composantes numériques indispensables à l'exercice de la profession correspondante. La formation ayant de plus en plus vocation à se mener tout au long de la vie, les dispositifs correspondants* [devraient] *également inclure des acquis de littératie numérique. Celle-ci* [devrait], *entre autres, permettre aux personnes qui n'ont pas ou peu bénéficié du système scolaire initial, d'acquérir les bases d'une culture numérique qui leur permette de vivre, travailler, et évoluer dans un monde de plus en plus numérique. Chaque personne en situation d'exclusion – précaire, migrant, sans-papiers, sans abri ou détenu… –,* [devrait] *pouvoir acquérir les bases indispensables de littératie numérique pour que le numérique ne devienne pas pour elle une double peine et facilite au contraire sa réinsertion sociale* » (3).

Recommandation n° 80

Afin de renforcer l'effectivité du droit d'accès à l'internet, instituer un droit pour chacun d'accéder à la « littératie » numérique.

B. LA NEUTRALITÉ DES RÉSEAUX : UN PRINCIPE À CONSACRER

Le débat sur la neutralité des réseaux porte sur la question de savoir quel contrôle les acteurs de l'internet responsables de l'acheminement du trafic ont le droit d'exercer sur le trafic acheminé pour des raisons à la fois techniques et économiques. Cette question doit être distinguée du débat relatif au contrôle de la puissance publique sur certains contenus illégaux acheminés sur internet (à travers notamment la problématique du blocage), alors que les deux questions sont souvent confondues dans le débat public.

---

(1) OCDE, La littératie à l'ère de l'information, *2000, p. 12.*

(2) Académie des sciences, L'enseignement de l'informatique en France : il est urgent de ne plus attendre, *mai 2013, p. 8.*

(3) Conseil national du numérique, Citoyens d'une société numérique, *novembre 2013, p. 39.*

Ce débat d'essence technico-économique a un impact important en matière de protection des droits fondamentaux. En effet, parce qu'elle permet à tout individu, toute entreprise ou toute association de bénéficier d'un égal accès à tous les internautes, la neutralité du net est, comme le droit d'accès, une garantie de la liberté d'expression, du droit à l'information, de la liberté d'entreprendre et de la liberté d'association.

Principe fondateur d'internet aujourd'hui menacé par l'évolution des pratiques des opérateurs de communications électroniques (**1**), la neutralité du net a fait l'objet d'un début de reconnaissance dans le droit positif mais il convient aujourd'hui d'aller plus loin dans sa consécration (**2**).

1. Un principe fondateur d'internet, aujourd'hui menacé par les pratiques des opérateurs

Pourtant fondateur d'internet (***a***), le principe de la neutralité des réseaux est aujourd'hui remis en cause par l'évolution des pratiques des opérateurs (***b***).

a. Un principe fondateur d'internet

Sur les plans techniques et philosophiques, internet a été conçu comme un réseau ouvert, reposant sur une architecture décentralisée et le principe du « meilleur effort » : chaque opérateur doit faire « de son mieux » pour assurer la transmission de tous les paquets de données qui transitent par son réseau, sans garantie de résultat mais en excluant toute discrimination à l'égard de la source, de la destination ou du contenu de l'information transmise. La neutralité du réseau est par conséquent **l'essence même du bien commun que constitue internet** et la condition de son développement et de son succès.

En 2003, dans le contexte du débat suscité aux États-Unis par les pratiques d'opérateurs de télécommunications qui entravaient l'accès de leurs abonnés à certains services ou à certaines applications, Tim Wu, universitaire américain qui en fut l'un des premiers théoriciens, rappelait que « *pour qu'un réseau public d'information soit le plus utile possible, il doit tendre à traiter tous les contenus, sites et plateformes de la même manière.* […] *Internet n'est pas parfait mais* ***son architecture d'origine tend vers ce but****. Sa nature décentralisée et essentiellement neutre est la raison de son succès à la fois économique et social* » [(1)].

C'est en effet en réponse à des pratiques des opérateurs de télécommunications tendant à remettre en cause ces fondamentaux techniques et philosophiques, que la neutralité des réseaux a commencé à être conceptualisée en tant que principe juridique à préserver.

---

(1) Tim Wu, extrait d'un article intitule « Network Neutrality, Broadband discrimination », in Open architecture as communications policy, *Center for Internet and society, Stanford Law School, 2004.*

b. Un principe menacé par l'évolution des pratiques des opérateurs

Depuis le début des années 2000, le trafic sur internet a connu une croissance exponentielle, d'abord sous l'effet du développement du *peer-to-peer*, puis de la vidéo. Cette évolution soulève des questions d'ordre technique liées à la gestion du trafic sur le réseau mais aussi des questions d'ordre économique portant sur la répartition des coûts engendrés par ce dernier entre les différents acteurs de l'internet et sur la répartition de la valeur entre les fournisseurs d'accès à internet et les fournisseurs de contenus. Dans ce contexte, les opérateurs de communications électroniques peuvent être tentés de mettre en place des pratiques susceptibles de remettre en cause la neutralité des réseaux (voir l'encadré ci-après).

Des pratiques risquant de remettre en cause la neutralité du réseau

(extrait du rapport sur la neutralité de l'internet remis au Gouvernement et au Parlement par l'Autorité de régulation des communications électroniques et des postes en septembre 2012)

« Les opérateurs tirent l'essentiel de leurs revenus de la vente du service d'accès à l'internet, grâce auquel les utilisateurs accèdent à des contenus et applications acheminés selon le principe du meilleur effort (« best effort »), indépendamment de leur nature, mais sans garantie de qualité. Par ailleurs, des services spécialisés sont proposés avec un niveau de qualité garantie contrôlé (comme la télévision et la vidéo à la demande proposées par les fournisseurs d'accès à l'internet, et certains services professionnels).

L'augmentation et la concentration du trafic, ainsi que le déploiement de nouveaux réseaux d'accès (fibre optique, réseau mobile de quatrième génération, etc.), se traduisent pour les opérateurs par des besoins de financement. Si ***de nouveaux revenus peuvent être recherchés au travers de nouveaux usages*** *– s'appuyant notamment sur des* ***services spécialisés*** *– les opérateurs cherchent par ailleurs à* ***augmenter la contribution des fournisseurs de contenus et d'applications au financement des réseaux****.*

Explorant de nouveaux modèles, les acteurs mettent en œuvre des pratiques susceptibles d'avoir des conséquences à long terme sur l'écosystème de l'internet. Des tendances telles que ***l'intégration verticale*** *de certains acteurs peuvent comporter des risques de discrimination anticoncurrentielle ou de réduction de la capacité d'innovation, par exemple. […]*

• ***Des opérateurs, pour contrôler la hausse du trafic, peuvent chercher à l'acheminer de manière différenciée****. Il s'agit des* ***pratiques de gestion de trafic****, qui peuvent consister à ralentir ou bloquer certaines catégories de contenus, ou au contraire à en prioriser d'autres. Elles sont susceptibles d'entraver, dans certaines circonstances, le principe de neutralité de l'internet. […]*

• ***Les pratiques de gestion de trafic*** *peuvent aussi viser à améliorer le niveau de qualité de service pour certaines catégories de contenus ou certains utilisateurs, ce qui peut toutefois se faire* ***au détriment de l'internet « best effort »****. Cette approche d'offres premium est d'autant plus efficace pour un FAI que la qualité de service associée à l'internet « best effort » est basse. Aussi importe-t-il d'en suivre le niveau afin de prévenir sa dégradation. […]*

• L'économie des relations entre acteurs de l'internet évolue rapidement. Le dimensionnement des liens et les flux financiers peuvent donner lieu à des tensions entre acteurs qui ne s'accordent pas sur ***les modalités d'interconnexion****. Des tendances telles que*

l'intégration verticale de certains acteurs peuvent comporter des risques de discrimination anticoncurrentielle ou de réduction de la capacité d'innovation par exemple ».

Source : ARCEP, Rapport au Parlement et au Gouvernement sur la neutralité de l'internet, Les actes de l'ARCEP, septembre 2012, pp 4-5.

Alors que la tentation est grande pour les fournisseurs d'accès à internet (FAI) de mettre en place une gestion différenciée des services, de vifs débats politiques ont lieu pour déterminer dans quelle mesure le principe de neutralité doit être garanti par la législation.

2. Un principe qui doit être plus clairement consacré dans le droit positif

Si le principe de la neutralité des réseaux a fait l'objet de premiers éléments de reconnaissance dans le droit positif (***a***), de vifs débats se font jour sur la définition qu'il convient d'en donner au niveau européen (***b***). Dans ce contexte, la Commission recommande de consacrer expressément ce principe dans une définition exigeante (***c***).

a. De premiers éléments de reconnaissance dans le droit positif

Alors que le principe de neutralité des réseaux fait l'objet de vives controverses aux États-Unis depuis le début des années 2000, c'est seulement à la fin des années 2000 que le débat a émergé en Europe.

En 2010, l'Autorité de régulation des communications électroniques et des postes (ARCEP) a formulé **dix recommandations non contraignantes** (voir l'encadré ci-après). En privilégiant le droit souple, la démarche générale se voulait alors avant tout préventive, l'Autorité estimant que les risques d'atteinte à la neutralité de l'internet portaient davantage sur des évolutions potentielles des pratiques que sur des dysfonctionnements avérés du marché.

Les 10 recommandations de l'ARCEP sur la neutralité de l'internet, septembre 2010

1. La liberté et la qualité dans l'accès à l'internet

L'Autorité recommande que le FAI qui propose un accès à l'internet soit tenu, dans le respect des dispositions législatives en vigueur, d'offrir à l'utilisateur final :

• la possibilité d'envoyer et de recevoir le contenu de son choix ;

• la possibilité d'utiliser les services ou de faire fonctionner les applications de son choix ;

• la possibilité de connecter le matériel et d'utiliser les programmes de son choix, dès lors qu'ils ne nuisent pas au réseau ;

• une qualité de service suffisante et transparente.

Des exceptions à ce principe sont possibles, sous réserve du respect du cadre prévu à la proposition n° 3.

2. La non-discrimination des flux dans l'accès à l'internet

Pour l'accès à l'internet, l'Autorité recommande que la règle générale soit de ne pas différencier les modalités de traitement de chaque flux individuel de données en fonction du type de contenu, de service, d'application, de terminal, ou en fonction de l'adresse

d'émission ou de réception du flux. Ceci s'applique en tout lieu du réseau, y compris à ses points d'interconnexion. Des exceptions à ce principe sont possibles, sous réserve du respect du cadre prévu à la proposition n° 3.

3. L'encadrement des mécanismes de gestion de trafic de l'accès à l'internet

Par exception aux principes posés dans les propositions n° 1 et n° 2, et afin que les éventuels écarts à ces principes restent limités, l'Autorité recommande que, lorsque des pratiques de gestion de trafic sont mises en place par les FAI pour assurer l'accès à l'internet, elles respectent les critères généraux de pertinence, de proportionnalité, d'efficacité, de non-discrimination des acteurs et de transparence.

4. Les services gérés

Afin de préserver la capacité d'innovation de l'ensemble des acteurs, tout opérateur de communications électroniques doit disposer de la possibilité de proposer, en complément de l'accès à l'internet, des « services gérés », aussi bien vis-à-vis des utilisateurs finals que des prestataires de services de la société de l'information (PSI), sous réserve que ces services gérés ne dégradent pas la qualité de l'accès à l'internet en deçà d'un niveau suffisant, ainsi que dans le respect du droit de la concurrence et des règles sectorielles.

5. La transparence accrue vis-à-vis des utilisateurs finals

Tant dans la présentation commerciale et les conditions contractuelles de leurs services de communications électroniques que dans les informations accessibles aux clients de ces offres en cours de contrat, les FAI doivent fournir à l'utilisateur final des informations claires, précises et pertinentes relatives aux services et applications accessibles via ces services ; à leur qualité de service ; à leurs limitations éventuelles ; ainsi qu'aux pratiques de gestion de trafic dont ils font l'objet.

À ce titre, l'Autorité recommande en particulier que :

• toute restriction d'un service de transmission de données par rapport aux principes de liberté d'usage et de non-discrimination des flux posés dans les propositions n° 1 et n° 2 soit explicitement indiquée dans la communication et dans les clauses contractuelles, de manière claire et compréhensible ;

• le terme « internet » ne puisse être utilisé pour qualifier ces services dès lors que certaines de ces restrictions ne seraient pas conformes aux exigences de la proposition n° 3 ;

• le terme « illimité » ne puisse être utilisé pour des offres de services incluant des limitations du type « usage raisonnable » ayant pour conséquence soit une coupure temporaire ou une facturation supplémentaire des services, soit une dégradation excessive des débits ou de la qualité de service.

6. Le suivi des pratiques de gestion de trafic

L'Autorité demandera aux FAI et associations qui les représentent, aux PSI et associations qui les représentent, ainsi qu'aux associations de consommateurs d'engager des travaux communs visant à identifier et qualifier les différents types de pratiques de gestion de trafic, y compris les limitations du type « usage raisonnable » associées aux offres dites « illimitées », et de lui faire part d'ici la fin du premier trimestre 2011 de leurs propositions à cet égard.

Dans le même temps, l'Autorité suivra l'évolution des pratiques de gestion de trafic mises en place par les opérateurs, afin d'apprécier en particulier le respect des critères de pertinence, d'efficacité, de proportionnalité, de non-discrimination des acteurs et de transparence.

7. Le suivi de la qualité de service de l'internet

Afin de veiller à ce que l'accès à l'internet présente une qualité de service suffisante et transparente, l'Autorité lancera des travaux visant à :

• qualifier les paramètres principaux de la qualité de service de l'accès à l'internet et élaborer des indicateurs adaptés ;

• faire publier périodiquement par les FAI de tels indicateurs de qualité de service de détail spécifiques aux services de transmission de données, notamment pour l'accès à l'internet, tant sur les réseaux fixes que mobiles.

8. Le suivi du marché de l'interconnexion de données

L'Autorité recommande :

• aux acteurs qui donnent aux utilisateurs finals l'accès à l'internet, de faire droit de manière objective et non discriminatoire à toute demande raisonnable d'interconnexion visant à rendre des services ou applications de l'internet accessibles à ces utilisateurs ;

• aux acteurs qui donnent aux PSI l'accès à l'internet, de faire droit de manière objective et non discriminatoire à toute demande raisonnable d'interconnexion visant à rendre les services ou applications de ces PSI accessibles à des utilisateurs de l'internet.

Cette recommandation s'accompagne d'une collecte périodique d'informations sur ces marchés.

9. La prise en compte du rôle des PSI dans la neutralité de l'internet

L'Autorité souligne que l'exercice effectif par les utilisateurs de leur liberté de choix entre les prestations (services/applications/contenus) rendues disponibles par les PSI via l'internet implique que ces derniers respectent :

• un principe de non-discrimination vis-à-vis des différents opérateurs pour l'accès à ces prestations ;

• des principes d'objectivité et de transparence vis-à-vis de l'utilisateur en ce qui concerne les règles utilisées, dans le cas où les PSI exercent un rôle de sélection ou de classement de contenus tiers, ce qui est notamment le cas des moteurs de recherche.

L'autorité invite les responsables privés et publics concernés à prendre pleinement en considération ces enjeux.

10. Le renforcement de la neutralité des terminaux

Dans le cadre de la révision prochaine de la directive RTTE, l'Autorité recommande que soit examinée l'opportunité de compléter cette directive pour mieux prendre en compte l'évolution du marché des terminaux, marqué notamment par l'importance croissante des couches logicielles et des interactions avec les PSI.

L'autorité invite les responsables privés et publics concernés à prendre pleinement en considération ces enjeux.

Source : ARCEP, Neutralité de l'internet et des réseaux. Propositions et recommandations, *Les actes de l'ARCEP, septembre 2010, pp 59-62.*

Si les préconisations du régulateur avaient le mérite d'identifier les menaces émergentes, elles ne constituent pas, aux yeux de la Commission, une digue suffisante pour protéger une conception exigeante de la neutralité.

C'est du droit de l'Union européenne que sont venus les premiers éléments de reconnaissance de la neutralité du net dans le droit positif. Dans le cadre de la transposition des directives européennes dites du « troisième paquet télécoms », l'ordonnance n° 2011-1012 du 24 août 2011 a ajouté à la liste des objectifs de la régulation des télécommunications, fixée par l'article L. 32-1 du code des postes et des communications électroniques, **deux objectifs liés à la neutralité du net**. L'ARCEP est ainsi désormais chargée :

– de veiller « *à l'absence de discrimination, dans des circonstances analogues, dans les relations entre opérateurs et fournisseurs de services de communication au public en ligne pour l'acheminement du trafic et l'accès à ces services* » ;

– et de « *favoriser la capacité des utilisateurs finals à accéder à l'information et à en diffuser ainsi qu'à accéder aux applications et services de leur choix* ».

L'ARCEP a également vu ses compétences accrues, en particulier en matière de règlements de différends. Ces derniers peuvent désormais concerner, en application de l'article L. 32-8 du même code, ceux portant sur les « *conditions réciproques techniques et tarifaires d'acheminement du trafic entre un opérateur et une entreprise fournissant des services de communication au public en ligne* » alors que l'ARCEP ne pouvait auparavant régler que les différends entre opérateurs. L'ARCEP peut aussi fixer des **exigences minimales** pour la qualité du service d'accès à internet, si cela apparaît nécessaire. La transposition a enfin renforcé les **obligations de transparence** qui s'imposent aux opérateurs, notamment en ce qui concerne leurs éventuelles pratiques de gestion de trafic.

Lors de son audition du 4 décembre 2014, M. Jean-Ludovic Silicani, alors président de l'ARCEP, a précisé **les outils dont l'Autorité dispose actuellement « *afin de mettre en œuvre progressivement le principe de neutralité de l'internet* »**.

En ce qui concerne l'interconnexion, il a rappelé que les relations entre les acteurs sont libres (voir l'encadré ci-après). L'interconnexion de données n'est pas régulée *ex ante*, c'est-à-dire que le régulateur n'a ni fixé de prescriptions applicables aux conditions techniques et financières de l'interconnexion, ni assigné d'obligation particulière à d'éventuels opérateurs puissants sur un marché donné. L'ARCEP peut toutefois, à tout moment, être saisie pour régler un différend entre deux opérateurs ou entre un opérateur et un fournisseur de contenus. Le bon exercice de cette compétence, étendue dans le cadre de la transposition des directives européennes de 2009, suppose un niveau suffisant de connaissance et de compréhension de l'état des marchés. Une décision du 29 mars 2012 prévoit, dans cette optique, la mise en œuvre d'une collecte périodique

d'informations sur les conditions techniques et tarifaires d'interconnexion et d'acheminement des données [1].

Le marché de l'interconnexion : enjeux pour la neutralité du net

L'interconnexion désigne la relation technico-économique qui s'établit entre des opérateurs ou entre des opérateurs et de grands fournisseurs de contenus pour se connecter et échanger mutuellement du trafic. Pour qu'un contenu parvienne à l'utilisateur final, il faut d'abord que le fournisseur de ce contenu, par exemple *Google*, s'interconnecte avec un opérateur de réseaux, par exemple *Orange*. Les conditions techniques et tarifaires de l'interconnexion font l'objet d'un contrat oral ou écrit. L'interconnexion peut être directe – ce que l'on appelle *peering* ou appairage – ou indirecte, *via* des transitaires, c'est-à-dire des courtiers qui servent d'intermédiaires entre opérateurs de réseaux et fournisseurs de contenus, tels qu'il en existe sur tous les marchés.

Dans le cadre de la préservation de la neutralité du net, une analyse approfondie de l'interconnexion s'impose. En effet, à l'origine, lorsque les flux de données étaient relativement limités et symétriques, l'interconnexion était gratuite. Cependant, sous l'effet de l'augmentation du trafic et des stratégies poursuivies par les différents acteurs, **le marché de l'interconnexion est le siège d'évolutions rapides**. Dans son rapport précité de septembre 2012, l'ARCEP relevait en particulier deux points de vigilance : **l'intégration verticale croissante des acteurs de ce marché** (diversification des FAI dans l'activité de transitaire, exercice simultané d'activités d'opérateur et de fournisseur de contenus) et **la volonté affichée par les FAI de faire contribuer financièrement les fournisseurs de contenus, via les conditions d'interconnexion** (par monétisation de l'interconnexion directe et le développement d'offres d'interconnexion différenciées payantes). Une telle évolution suscite **des tensions entre catégories d'acteurs**. Or, un échec des négociations entre deux acteurs interconnectés pourrait conduire à la dégradation ou la rupture de l'interconnexion et rendre impossible aux utilisateurs l'accès, la diffusion ou l'utilisation des applications et services de leur choix. Par ailleurs, **l'interconnexion peut être utilisée dans une optique de discrimination anticoncurrentielle à l'égard de la source, de la destination ou du contenu de l'information transmise**. Il convient donc d'être vigilant quant au développement de telles pratiques.

En 2011, l'Autorité de la concurrence a été saisie d'un différend entre *Cogent* et *France Télécom* en matière d'interconnexion de trafic internet. La société *Cogent* réclamait l'ouverture par *France Télécom* de nouvelles capacités de *peering*. *France Télécom* exigeait une contrepartie financière compte tenu des déséquilibres de trafic, alors que *Cogent* estimait que *France Télécom* détenait une infrastructure essentielle et devait par conséquent fournir la capacité sans contrepartie financière. L'autorité a conclu que *France Télécom* ne détenait pas d'infrastructure essentielle, mais que, compte tenu de sa position dominante sur « *le marché des offres d'accès direct ou indirect aux abonnés français du fournisseur d'accès à Internet Orange* » [1], France Télécom devait appliquer des conditions non-discriminatoires à l'égard de ses partenaires commerciaux, notamment par rapport aux conditions qu'elle applique à ses propres services et filiales. La décision de l'Autorité de la concurrence a été confirmée par la cour d'appel de Paris [2] et par la Cour de cassation [3].

(1) Décision n° 12-D-18 du 20 septembre 2012.

(2) Cour d'appel de Paris, 19 décembre 2013.

(3) Cass. com., 12 mai 2015, n° 14-10.792.

---

(1) La décision de l'ARCEP mettant en place cette collecte d'informations a fait l'objet d'un recours des sociétés ATT *et* Verizon, *recours rejeté par le Conseil d'État le 10 juillet 2013,* Société AT&T Global Network Services France SAS et autres, *n° 360397.*

Comme l'a rappelé M. Jean-Ludovic Silicani lors de son audition, **les conditions de l'interconnexion doivent être transparentes et non discriminatoires**. « *L'absence de discrimination signifie que, si un opérateur de réseaux fait payer un grand acteur de l'internet pour accéder à son réseau, il devra également faire payer les autres acteurs de taille comparable. De même, s'il accorde à un petit acteur de l'internet l'accès gratuit à son réseau, il ne pourra pas le refuser à d'autres petits acteurs. Le principe de non-discrimination impose en effet de traiter de la même manière des acteurs qui se trouvent dans une situation similaire, mais il n'interdit pas de traiter de manière différente des acteurs qui sont dans des situations différentes* ». Sur le fondement de sa décision de mars 2012, **l'ARCEP surveille le marché de l'interconnexion et s'assure que ces principes sont respectés**.

Une fois le stade de l'interconnexion franchi, le principe de neutralité s'applique à l'acheminement du contenu jusqu'à l'utilisateur final. À cet égard, il convient de distinguer deux modes d'acheminement : *via* le service général d'accès à internet ou *via* des services spécialisés.

En ce qui concerne le service général d'accès à internet, le principe de neutralité s'applique strictement : le FAI ne peut pratiquer aucune discrimination dans la façon dont il achemine les différents contenus sur son réseau jusqu'à l'utilisateur final. En d'autres termes, il ne peut privilégier aucun contenu par rapport à un autre. Néanmoins, il est autorisé à mettre en place une gestion technique du trafic de manière à éviter des « embouteillages », dès lors qu'il l'applique de la même manière à tous les contenus. La règle qui prévaut est celle du *best effort* : il n'y a pas de qualité garantie, mais le FAI doit acheminer tous les contenus du mieux qu'il peut, compte tenu des investissements qu'il a réalisés pour disposer de « tuyaux » efficaces du point de vue quantitatif et qualitatif. Plus le FAI investit, meilleure est la qualité générale du trafic sur l'internet.

En matière de « régulation » des services spécialisés, l'ARCEP utilise le pouvoir de surveillance de la qualité du service général d'accès à l'internet que lui a donné le cadre européen transposé dans la loi française afin de s'assurer que le fonctionnement général d'internet ne se dégrade pas, compte tenu du partage entre ce service général et les services spécialisés (voir l'encadré ci-après).

Les services spécialisés : enjeux pour la neutralité du net

Les services, dits spécialisés ou gérés, offerts par les opérateurs, ne font pas partie de l'internet général. À la différence du service général d'accès à l'internet, ils font l'objet d'un contrat entre un fournisseur de contenus – par exemple, *France Télévisions*, *Google ou Netflix* – et un FAI – par exemple, *Orange*. Celui-ci achemine le contenu jusqu'à l'utilisateur final en **garantissant une certaine qualité de service, moyennant une rémunération**. La télévision ou la téléphonie, proposées dans les offres « triple play » sont autant de services gérés ou spécialisés : ils sont délivrés sur des canaux dédiés, fonctionnent en vase clos et ne pâtissent pas d'un réseau qui peut être temporairement surchargé ou inaccessible. S'agissant de services *premium*, **l'opérateur gère le service de bout en bout et peut garantir une qualité de service**. Ce n'est pas le cas de l'internet commun, qui est caractérisé par son fonctionnement selon le principe du meilleur effort. Au-delà de la téléphonie et de la

télévision, les services gérés peuvent concerner la télémédecine, le vote en ligne ou d'autres usages innovants. **Les opérateurs de communications électroniques souhaitent développer ces services afin de dégager de nouveaux revenus**.

Se pose la question de savoir dans quelles conditions le service général d'accès à internet et les services spécialisés peuvent cohabiter. Ainsi, comme l'a rappelé M. Jean-Ludovic Silicani, lors de son audition du 4 décembre 2014, « ***il existe un risque indéniable que les services spécialisés à qualité de service garantie finissent, du fait de leur multiplication, par écraser la qualité de l'accès général à internet***. *À ce stade, en France, ce risque n'est pas d'actualité, compte tenu de l'importance des investissements réalisés dans les réseaux fixes – notons que les mêmes questions se poseront pour les réseaux mobiles, mais seulement dans quelques années. Néanmoins, il pourrait se matérialiser si les services spécialisés étaient multipliés par dix* ».

Une décision générale du 29 janvier 2013 a défini les conditions dans lesquelles l'ARCEP mesure la qualité du service général d'accès à internet. Sur cette base, l'ARCEP a publié en novembre 2014 les premières mesures de la qualité du service fixe d'accès à l'internet. Lors de son audition du 4 décembre 2014, M. Jean-Ludovic Silicani a néanmoins souligné qu'il convenait de rester très prudent quant à l'interprétation de ces résultats, la méthode nécessitant encore d'être consolidée, vérifiée et précisée.

Comme l'a rappelé l'ancien président de l'ARCEP, si cette dernière, sur la base de ces mesures, « *constatait que la qualité du service général d'accès à internet se dégrade ou que, sans se détériorer, elle est inférieure à un niveau standard, elle pourrait d'abord rechercher les causes de ce phénomène. Ensuite, elle pourrait prendre des mesures. Par exemple, si elle établissait que la qualité d'accès général à l'internet offerte par un opérateur est insuffisante – compte tenu de ce qu'elle a été, de la moyenne du marché et de ce qu'on peut estimer nécessaire au moment considéré –,* ***elle pourrait interdire à cet opérateur de s'appeler FAI****. Ce premier outil, qui peut sembler banal, est en réalité très puissant : son utilisation peut entraîner la mort de l'opérateur. Nous ne pouvons pas prévoir aujourd'hui si nous aurons besoin d'y recourir, mais il est important qu'il existe* ».

M. Jean-Ludovic Silicani a également souligné que **la concurrence constitue un deuxième outil de régulation des services gérés**. « *Sur un marché peu concurrentiel, l'internaute a le choix entre un nombre limité de FAI. Si la qualité de l'accès à l'internet offerte par ces FAI se dégrade, il ne pourra que subir cette situation. En revanche, sur un marché concurrentiel, si l'internaute constate une telle dégradation et que l'ARCEP l'attribue, le cas échéant, à une multiplication excessive des services spécialisés, il pourra changer de FAI, en en choisissant un qui apporte une qualité de service satisfaisante. C'est l'une des vertus de la concurrence. Ainsi, le consommateur a un rôle actif à jouer pour que le marché fonctionne bien. Celui-ci s'autorégule grâce à l'addition des choix individuels des internautes* ».

S'il existe donc de premières réponses dans le droit existant, certains exigent d'aller plus loin dans la protection juridique de la neutralité des

réseaux. Se pose notamment la question d'une consécration plus explicite et plus protectrice du principe de neutralité du net et notamment d'une définition plus stricte des cas limitatifs dans lesquels il est possible de déroger à ce principe. Au plan national, les propositions formulées par des parlementaires tendant aller plus loin en inscrivant le principe de neutralité du net dans la loi n'ont pas abouti [(1)]. Ces questions font actuellement débat au niveau européen puisque c'est à nouveau du droit de l'Union européenne que devrait venir une consécration du principe de neutralité du net.

b. Les débats sur la définition du principe à consacrer au plan européen

La proposition de règlement établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté, adoptée par la Commission européenne le 11 septembre 2013 et qualifiée de « **quatrième paquet télécoms** », comporte une reconnaissance plus large du principe de neutralité du net. Son article 24 **consacre le principe dans des termes très proches de ceux des recommandations établies par l'ARCEP en 2010 mais en leur donnant une portée contraignante**.

La définition qu'il convient de donner à la neutralité du net donne néanmoins lieu à d'importants débats, portant en particulier sur la marge de manœuvre à laisser aux fournisseurs d'accès à internet pour déroger à ce principe. À cet égard, le Parlement européen a adopté la proposition de règlement en première lecture le 3 avril 2014 dans des termes plus protecteurs de la neutralité (voir l'encadré ci-après).

En ce qui concerne la possibilité de pratiquer des **mesures techniques de gestion de trafic**, le texte voté par le Parlement est plus exigeant que la proposition de la Commission. Il supprime en effet la possibilité de mesures de gestion de trafic destinées à prévenir les communications non sollicitées et exige que la congestion du trafic justifiant une mesure de gestion soit « temporaire et exceptionnelle », alors que la proposition de la Commission parlait de congestion « temporaire ou exceptionnelle ».

La définition des services gérés fait également l'objet d'un important débat, en particulier quant à la définition qu'il convient de leur donner.

Le texte voté par la Commission européenne apparaissait à cet égard particulièrement souple : tout service faisant l'objet d'un accord tendant à garantir sa qualité était qualifié de service spécialisé. Dès lors, le développement des services gérés aurait été rendu possible dans une ampleur susceptible de remettre en cause la qualité générale d'internet.

---

(1) Proposition de loi n° 3061 relative à la neutralité de l'Internet, présentée par MM. Jean-Marc Ayrault, Christian Paul et al., déposée sur le Bureau de l'Assemblée nationale le 20 décembre 2010 *; proposition de loi n° 190 relative à la neutralité de l'Internet, présentée par Mme Laure de la Raudière, déposée sur le Bureau de l'Assemblée nationale le 12 septembre 2012.*

Le Parlement a d'une part précisé que la « qualité supérieure » des services gérés devait être nécessitée par la fonctionnalité du service. D'autre part, alors que la proposition de la Commission exigeait seulement que la fourniture des services gérés « *ne porte pas atteinte d'une manière récurrente et continue à la qualité générale des services d'accès à l'internet* », le texte du Parlement exige qu'elle ne porte pas atteinte à la disponibilité ou à la qualité des services d'accès à internet.

La neutralité du net définie par le projet de règlement dans sa rédaction votée par le Parlement européen le 3 avril 2014

Article 2. 12 *bis* : « *Neutralité de l'internet, le principe selon lequel l'ensemble du trafic internet est traité de façon égale, sans discrimination, limitation ni interférence, indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application* ».

Article 23. 1 : *« Les utilisateurs finaux ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'exécuter et de fournir les applications et les services et d'utiliser les terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, ou quels que soient le lieu, l'origine ou la destination du service, de l'information ou du contenu, par l'intermédiaire de leur service d'accès à internet* ».

2. « *Les fournisseurs d'accès à internet, les fournisseurs de communications électroniques au public et les fournisseurs de contenus, d'applications et de services sont libres de proposer des services spécialisés aux utilisateurs finaux. Ces services ne sont proposés que si la capacité du réseau est suffisante pour les fournir en plus des services d'accès à l'internet et s'ils ne portent pas atteinte à la disponibilité ou à la qualité des services d'accès à internet. Les fournisseurs proposant un accès à l'internet aux utilisateurs finaux n'opèrent pas de discrimination entre des services ou des applications fonctionnellement équivalents* ».

La définition proposée par le Parlement a été critiquée, notamment par les opérateurs de télécommunications, comme étant trop restrictive et comme risquant de faire obstacle à l'innovation. L'ancien président de l'ARCEP, lors de son audition du 4 décembre 2014, a souligné, s'agissant des services spécialisés, qu'« *une majorité d'États membres, dont la France, est favorable à une solution intermédiaire entre la position probablement trop souple de la Commission et celle, trop rigide, du Parlement. (...) L'intérêt des services spécialisés est, au demeurant, de favoriser l'innovation. Il convient donc de trouver le bon équilibre entre le laisser-faire, qui nous amènerait à tolérer des situations inacceptables, et la fixation de règles trop rigides qui deviendraient vite obsolètes et, donc, inapplicables, voire un excès d'intervention qui dissuaderait l'innovation* ».

Le Conseil d'État, dans son étude annuelle 2014, estime lui aussi que « *la consécration du principe de neutralité des réseaux apparaît particulièrement nécessaire aujourd'hui* » mais que « *le projet de règlement dans sa rédaction votée par le Parlement européen le 3 avril 2014, apparaît excessivement restrictif* » [(1)]. C'est pourquoi il préconise l'inscription dans la loi et le règlement

(1) Conseil d'État, op. cit., *pp. 270-271.*

de l'Union européenne du principe de neutralité des opérateurs de communications électroniques dans les termes votés par le Parlement européen le 3 avril 2014, sous trois réserves importantes :

– revenir à la définition plus souple des mesures de gestion de trafic de la proposition de la Commission ;

– revenir à la définition plus large des « services spécialisés ». Pour le Conseil d'État, « *il serait souhaitable que des services de qualité supérieure se développent même si un tel degré d'exigence n'est pas strictement nécessaire au service* ». Le choix d'une définition plus large doit en revanche, selon le Conseil, s'accompagner de garanties plus fermes concernant l'absence de dégradation de la qualité générale d'internet : information préalable de l'autorité de régulation concernée sur le projet de convention ; droit d'opposition de l'autorité en cas de risque manifeste de dégradation de la qualité de l'internet en-deçà d'un niveau satisfaisant ; contrôle en continu par l'autorité de la qualité de l'accès à internet et droit de suspension de l'autorité de régulation s'il s'avère que la qualité de l'internet est dégradée.

– et permettre aux opérateurs d'exiger un paiement des fournisseurs de contenus les plus importants pour ne pas voir leur qualité d'accès dégradée, dans le cadre d'une facturation asymétrique.

Le président de l'ARCEP a lui aussi plaidé en faveur d'une définition souple des services gérés laissant d'importantes marges d'appréciation au régulateur : « *Nous pensons qu'il n'est guère utile de définir par écrit les cas limitatifs dans lesquels les services spécialisés peuvent être créés car, dans ces domaines où la technologie et les usages évoluent très rapidement, nous serons toujours dépassés : ce que nous écrivons un jour risque d'être privé de sens et de portée le lendemain. Néanmoins, nous devons veiller à ce que la qualité de l'accès général à l'internet ne se dégrade pas en raison d'un excès de services spécialisés, et nous disposons d'outils à cette fin. Telle est la méthode que nous préconisons. Dans son étude sur le numérique, le Conseil d'État a proposé que tout nouveau service spécialisé établi entre un opérateur de télécommunications et un fournisseur de contenus soit déclaré auprès de l'ARCEP – les opérateurs de télécommunications en tant que tels sont déjà soumis à une telle obligation de déclaration. Cela nous paraît une bonne formule.* (…) *L'innovation étant permanente dans ce domaine, ce que nous écrivons aujourd'hui risque d'être démenti demain. Mieux vaut fixer de grands principes, des valeurs, des caps, tout en restant pragmatique dans leur mise en œuvre. Oui à un cadre législatif général, mais en laissant des marges de manœuvre au régulateur dont c'est là une des raisons d'être* ».

En revanche, dans son rapport au Premier ministre de juin 2015, *Ambition numérique*, le Conseil national du numérique se prononce en faveur de l'inscription dans le droit de la définition adoptée par le Parlement européen le 3 avril 2014.

Le 30 juin 2015, après des mois de négociation, la Commission européenne a annoncé avoir trouvé un accord avec le Parlement européen et le Conseil sur la révision du « quatrième paquet télécom ». Cet accord présente de nombreuses améliorations par rapport au texte proposé initialement par la Commission mais il est en retrait par rapport à celui présenté par le Parlement sur certains points :

– le texte de compromis supprime formellement la notion de « ***neutralité de l'internet*** » pour viser un « *traitement équitable et non discriminatoire du trafic* » et la remplace par la référence à « ***l'accès à un internet ouvert*** » ;

– en matière de **gestion de trafic**, alors que le texte du Parlement exigeait que la congestion du trafic soit « *temporaire* et *exceptionnelle* », le compromis revient à la rédaction initiale de la Commission évoquant une congestion « ***temporaire* ou *exceptionnelle*** » ; en revanche, le compromis confirme la suppression par le Parlement des mesures de gestion destinées à prévenir la transmission de communications non sollicitées ;

– s'agissant des **« services spécialisés »**, si le texte final ne retient pas la définition exigeante posée par le Parlement (« *optimisé pour des contenus, applications ou services spécifiques, ou une combinaison de ceux-ci, fourni au travers de capacités logiquement distinctes, reposant sur un contrôle strict des accès, offrant une fonctionnalité nécessitant une qualité supérieure de bout en bout* »), il précise que ces services doivent être « *optimisés pour des contenus, des applications ou des services spécifiques, ou une combinaison de ceux-ci, lorsque l'optimisation est nécessaire pour faire en sorte que les contenus, les applications ou les services satisfassent à un niveau de qualité donné* » ; il conserve en revanche l'exigence de **maintien de la disponibilité ou de la qualité générale des services d'accès à l'internet** comme l'avait précisé le Parlement.

Compromis final en vue d'un accord sur la proposition de règlement établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté (extraits)

L'**article 1er** définit ainsi l'exigence de **traitement égal et non discriminatoire du trafic** : *« le présent règlement établit des règles communes destinées à garantir **le traitement équitable et non-discriminatoire du trafic dans le cadre de la fourniture de services d'accès à l'internet et à préserver les droits connexes des utilisateurs finals.** (...)* ». Cette définition vise à suppléer la **suppression de la définition de la neutralité de l'internet à l'article 2**, remplacée, dans d'autres parties de la proposition de règlement, par l'expression « ***internet ouvert*** ». La référence à la notion de « *service spécialisé* », par opposition à « *service d'accès à l'internet* » est transférée à l'article 3.5.

L'**article 3** fixe les **modalités de « l'accès à un internet ouvert »,** c'est-à-dire la possibilité pour les FAI de conclure des accords avec les utilisateurs finaux pour fixer des **règles commerciales et techniques spécifiques sur l'accès à internet en matière de prix, de volume et de vitesse (§2)**, les conditions à la mise en œuvre de

mesures de gestion du trafic (§3) et la possibilité pour les fournisseurs de communications électroniques de proposer des « **services spécialisés** » **(§5)** :

« 1. Les utilisateurs finals ont le ***droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir les applications et les services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination du service, de l'information ou du contenu, par l'intermédiaire de leur service d'accès à l'internet.***

« Le présent paragraphe s'entend sans préjudice du droit de l'Union et du droit national conforme au droit de l'Union concernant la légalité des contenus, des applications et des services.

« 2. ***Les accords entre les fournisseurs de services d'accès à l'internet et les utilisateurs finals*** *relatifs aux conditions commerciales et techniques et aux caractéristiques des services d'accès à l'internet, telles que les* ***prix****, les* ***volumes*** *de données* ***ou*** *le* ***débit, et les pratiques commerciales utilisées par les fournisseurs de services d'accès à l'internet ne limitent pas l'exercice par les utilisateurs finals des droits visés au paragraphe 1.***

« 3. Dans le cadre de la fourniture de services d'accès à l'internet, les fournisseurs ***traitent le trafic de façon égale et sans discrimination, restriction ni interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis et les équipements terminaux utilisés.***

« Le premier alinéa n'empêche pas les fournisseurs de services d'accès à l'internet d'appliquer des ***mesures de gestion raisonnable du trafic.*** *Pour être réputées raisonnables, les mesures sont* ***transparentes, non discriminatoires et proportionnées*** *et elles sont* ***fondées non sur des considérations commerciales mais sur des différences objectives entre les exigences techniques en matière de qualité de service de certaines catégories spécifiques de trafic. Ces mesures n'impliquent pas une surveillance du contenu particulier et ne sont pas maintenues plus longtemps que nécessaire.***

« ***Les fournisseurs de services d'accès à l'internet*** *n'appliquent pas de mesures de gestion du trafic qui aillent au-delà des mesures visées au deuxième alinéa et, en particulier,* ***s'abstiennent de bloquer, de ralentir, de modifier, de restreindre, de perturber, de dégrader ou de traiter de manière discriminatoire des contenus, des applications ou des services***

particuliers ou certaines catégories particulières de contenus, d'applications ou de services, si ce n'est dans la mesure nécessaire et seulement le temps nécessaire, pour *:*

« a) ***se conformer à la législation de l'Union ou à la législation nationale conforme au droit de l'Union*** *à laquelle le fournisseur de services d'accès à l'internet est soumis ou aux modalités d'exécution de ces législations, y compris les décisions d'un tribunal ou d'une autorité publique investie de pouvoirs d'exécution ;*

« b) ***préserver l'intégrité et la sûreté du réseau, des services fournis par l'intermédiaire de ce réseau et des équipements terminaux*** *des utilisateurs finals ;*

« c) ***prévenir une congestion imminente du réseau et atténuer les effets d'une congestion temporaire ou exceptionnelle du réseau****, pour autant que les catégories équivalentes de trafic fassent l'objet d'un traitement identique.*

« (...)

« 5. ***Les fournisseurs de communications électroniques au public****, y compris les fournisseurs de services d'accès à l'internet et les fournisseurs de contenus, d'applications et de services* ***sont libres de proposer des services autres que les services d'accès à l'internet qui sont optimisés pour des contenus, des applications ou des services spécifiques, ou une combinaison de ceux-ci, lorsque l'optimisation est nécessaire pour***

faire en sorte que les contenus, les applications ou les services satisfassent à un niveau de qualité donné.

« Les fournisseurs de communications électroniques au public, y compris les fournisseurs de services d'accès à l'internet, peuvent proposer ou faciliter ce type de services ***uniquement si les capacités du réseau sont suffisantes pour permettre de les fournir en plus des services d'accès à l'internet déjà fournis.*** *Ces services ne* ***sont pas utilisables comme services d'accès à l'internet ni proposés en remplacement de ces derniers,*** *et ils ne sont* ***pas proposés au détriment de la disponibilité ou de la qualité générale des services d'accès à l'internet*** *pour les utilisateurs finals ».*

L'article 4 traite des mesures de surveillance, d'exécution et de transparence destinées à garantir l'accès à un internet ouvert. Il dispose notamment que « ***les autorités réglementaires nationales surveillent étroitement et garantissent la conformité à l'article 3*** *et aux paragraphes 3 à 6 du présent article,* ***et encouragent le maintien d'un accès à l'internet non discriminatoire à des niveaux de qualité qui correspondent à l'état des technologies****. À cette fin, les autorités réglementaires nationales* ***peuvent imposer des caractéristiques techniques, des exigences minimales de qualité du service et d'autres mesures appropriées et nécessaires à un ou plusieurs fournisseurs de communications électroniques au public****, y compris les fournisseurs de services d'accès à l'internet. Elles publient tous les ans des rapports sur la surveillance qu'elles exercent et sur leurs constatations et remettent ces rapports à la Commission et à l'ORECE ».*

c. Consacrer clairement le principe de neutralité du net dans une définition exigeante

De prime abord, la Commission souhaite que soit privilégiée une **stratégie juridique de prévention des atteintes au principe de neutralité du net par l'inscription du principe dans la loi**, plutôt qu'une réparation correctrice qui serait illusoire. Ainsi que l'énoncent de manière générale et positive les considérants du texte de compromis final précité, le principe de neutralité de l'internet doit garantir un traitement égal et non-discriminatoire du trafic par les fournisseurs de services d'accès à internet et préserver les droits des utilisateurs de ces réseaux de pouvoir, à travers leur service d'accès à internet, accéder aux informations et aux contenus qu'ils souhaitent, les diffuser et utiliser ou fournir les applications et les services de leur choix sans aucune discrimination. Elle propose de le consacrer en droit positif **en le définissant comme le traitement égal, non-discriminatoire et sans restriction ou interférence de l'ensemble du trafic, quels que soient l'expéditeur, le destinataire, le contenu, l'appareil, le service ou l'application**.

Recommandation n° 81

Consacrer dans la loi ou le règlement de l'Union européenne le principe de neutralité des opérateurs de communications électroniques dans la définition suivante : un traitement égal et sans discrimination, restriction ni interférence de l'ensemble du trafic, quels que soient l'expéditeur ou le destinataire, le contenu consulté ou diffusé, l'application ou le service utilisés ou fournis et les équipements terminaux utilisés.

Ce principe général doit se traduire par plusieurs garanties spécifiques.

Tout d'abord, l'**accès à un internet ouvert** doit être préservé, ce qui suppose, d'une part, une **liberté de choix** par les utilisateurs finals **des équipements terminaux et des technologies de réseau** et, d'autre part, un **contrôle des accords et pratiques commerciales qui régissent le volume de données, le débit et le tarif**.

Recommandation n° 82

Préserver l'accès à un internet ouvert en instaurant une liberté de choix des terminaux et des technologies de réseau par les utilisateurs finals et un contrôle des accords et pratiques commerciales qui régissent le volume de données, le débit et le tarif.

Ensuite et par dérogation au principe du traitement égal, non-discriminatoire et sans restriction ou interférence de l'ensemble trafic, **des mesures de gestion du trafic sont possibles mais doivent être raisonnables**, **transparentes**, **proportionnées**, **non-discriminatoires et fondées** non sur des considérations commerciales mais **sur des différences objectives entre catégories de trafic équivalentes**. En outre, **elles ne doivent pas conduire à bloquer, ralentir, modifier, restreindre, perturber, dégrader ou traiter de manière discriminatoire certains contenus, applications ou services, sauf si c'est strictement nécessaire à l'un des objectifs précisément et clairement définis par le législateur**. Parmi ces objectifs peuvent figurer **l'obligation d'exécuter une décision de justice**, la **préservation de l'intégrité et de la sûreté du réseau** ainsi que **la prévention d'une congestion imminente du réseau ou l'atténuation des effets d'une congestion temporaire *ou* exceptionnelle**, à condition de traiter de manière identique des catégories de trafic équivalentes.

Recommandation n° 83

N'autoriser les mesures de gestion du trafic que si :

– elles sont raisonnables, transparentes, proportionnées, non-discriminatoires et fondées sur des différences objectives entre catégories de trafic équivalentes ;

– elles ne conduisent pas à bloquer, ralentir, modifier, restreindre, perturber, dégrader ou traiter de manière discriminatoire certains contenus, applications ou services, sauf si elles visent à satisfaire une obligation précisément et clairement définie par le législateur (exécution d'une décision de justice, préservation de l'intégrité et de la sûreté du réseau, prévention d'une congestion imminente du réseau ou atténuation des effets d'une congestion temporaire *ou* exceptionnelle).

Par ailleurs, **les « services spécialisés », susceptibles de porter atteinte à la qualité générale d'internet, doivent faire l'objet d'un encadrement strict**. S'il est loisible aux fournisseurs d'accès de conclure des contrats avec des fournisseurs de contenus, d'applications et de services pour lesquels une qualité de service supérieure à celle de l'internet général est garantie, ils ne sauraient le faire sans se conformer à certaines obligations.

D'une part, **l'optimisation de ces « services spécialisés » doit répondre objectivement aux caractéristiques spécifiques et essentielles du contenu, de l'application ou du service concerné et nécessiter leur fourniture à un certain niveau de qualité**.

D'autre part, **ces « services spécialisés » ne doivent pas être fournis au détriment de la disponibilité ou de la qualité générale des services d'accès à l'internet ni être proposés en remplacement de ces derniers**. À l'instar de ce qu'a proposé M. Jean-Ludovic Silicani lors de son audition et le Conseil d'État dans son étude annuelle [(1)], la Commission recommande de **prévoir la notification préalable à l'ARCEP de tout accord conclu entre les fournisseurs de contenus, d'applications et de services et les opérateurs de communications électroniques portant sur des « services spécialisés » afin que cette autorité puisse s'y opposer en cas de risque de dégradation de la qualité du service général d'accès à l'internet**.

Recommandation n° 84

Encadrer strictement le développement des « services spécialisés » :

– l'optimisation de ces services doit répondre objectivement aux caractéristiques spécifiques et essentielles du contenu, de l'application ou du service concerné et nécessiter leur fourniture à un certain niveau de qualité ;

– ils ne doivent pas être fournis au détriment de la disponibilité ou de la qualité générale des services d'accès à l'internet ni être proposés en remplacement de ces derniers ;

– prévoir la notification préalable à l'ARCEP de tout accord conclu entre les fournisseurs de contenus, d'applications et de services et les opérateurs de communications électroniques portant sur ce type de services afin qu'elle puisse s'y opposer en cas de risque de dégradation de la qualité du service général d'accès à l'internet.

Enfin, une dernière condition pratique de l'exercice des libertés numériques consiste à **disposer d'un terminal** – ordinateur, tablette, téléphone

(1) Conseil d'État, op. cit., *pp. 270-272.*

portable – « **de confiance »**, **permettant à son utilisateur d'exécuter toutes les tâches qu'il souhaite et de n'en accomplir aucune sans son consentement**.

Or, la réalité est aujourd'hui bien différente et les exemples ne manquent pas pour en témoigner. La dernière version de *Windows* a suscité de vives polémiques en raison du caractère massif de la collecte de données opérée par ce système d'exploitation à l'insu de ses utilisateurs. De même la société *Apple* exclut-elle régulièrement certaines applications de son *Appstore* au motif qu'elles contreviendraient aux règles draconiennes qu'elle a fixées en termes de concurrence ou de mœurs. Enfin, des fonctionnalités inconnues de l'utilisateur légitime (« portes dérobées » ou « *backdoors* ») sont régulièrement découvertes dans les principaux systèmes d'exploitation grand public, permettant leur piratage. Il semble donc nécessaire de renforcer les garanties entourant la conception et l'utilisation tant du matériel que du système d'exploitation ou encore des logiciels sans oublier, dans le cas des terminaux mobiles, des « magasins d'applications » qui exercent un contrôle étroit sur l'accès du plus grand nombre aux logiciels.

Les protections nécessaires ne relevant pas toutes du droit positif, une **réponse multiforme** doit être apportée à ce problème complexe, à commencer par **l'encouragement à la production et à l'usage de « biens communs informationnels »** (comme les logiciels libres), **le soutien des fabricants et éditeurs européens**, **l'instauration d'exigences d'interopérabilité et de contrôles des logiciels utilisés par le secteur public ou la pleine mobilisation des autorités de contrôle en matière de respect de la vie privée, de sécurité des systèmes d'information et de concurrence**.

Recommandation n° 85

Créer les conditions pour qu'un utilisateur dispose d'un terminal « de confiance » lui permettant d'exécuter toutes les tâches qu'il souhaite et de n'en accomplir aucune sans son consentement. À cette fin, privilégier une approche multiforme : encouragement à la production et à l'usage de « biens communs informationnels » (comme les logiciels libres), soutien des fabricants et éditeurs européens, instauration d'exigences d'interopérabilité et de contrôles des logiciels utilisés par le secteur public, mobilisation des autorités de contrôle en matière de respect de la vie privée, de sécurité des systèmes d'information et de concurrence…

Le Conseil national du numérique alerte aussi sur le risque que les accords de transit et de *peering* négociés entre opérateurs d'infrastructures et fournisseurs de contenus et d'application ne constituent « *un cheval de Troie d'une atteinte à la neutralité du net* ».

S'agissant du marché de l'interconnexion, comme l'a rappelé M. Jean-Ludovic Silicani, ancien président de l'ARCEP lors de son audition, « *il existe une grande différence entre la France et les autres pays puisque nous estimons – et nous l'avons écrit dans nos recommandations – que le principe de*

neutralité s'applique dès l'interconnexion. Ce n'est pas le cas aux États-Unis, même aux yeux de la FCC : la neutralité ne concerne que l'acheminement ultérieur. En d'autres termes, la France a une définition plus large de la neutralité, affirmée par le régulateur et partagée, je crois, par les parlementaires et les experts qui suivent ces questions. (...) C'est pourquoi ***nous menons une action préventive de surveillance de ce marché****, afin de connaître ce qui s'y passe, de quantifier les flux de trafic et les flux financiers auxquels il donne lieu et de vérifier qu'il n'y a pas d'anomalies. Si nous constations des dérapages significatifs mettant le système en péril, nous pourrions aller plus loin et mettre en place une régulation. Encore faudrait-il que nous ayons une base légale pour le faire, et, à l'heure actuelle, la Commission européenne n'y est pas prête. Cela supposerait soit une solution nationale – mais le Parlement pourrait-il l'adopter sans méconnaître le droit communautaire ? –, soit un consensus au niveau de l'Union européenne pour réguler. Pour le moment, nous n'en sommes qu'au stade de la prévention, pas à celui de la « guérison » ou de la sanction* » (1).

Le Conseil national du numérique propose de conférer à l'ARCEP un « *droit de regard sur les accords de* peering *et de transit* » permettant de s'assurer « *que ces accords ne sont pas sources de déséquilibres dans le traitement des contenus, en particulier au profit des acteurs puissants* » (2). La Commission souscrit à cette proposition d'un renforcement du contrôle de l'ARCEP sur le marché de l'interconnexion.

Recommandation n° 86

Renforcer le contrôle de l'ARCEP sur le marché de l'interconnexion.

De manière générale, la Commission appelle de ses vœux **un renforcement de la transparence** sur les performances techniques des offres d'accès à internet, les risques de congestion des réseaux, les pratiques de gestion de trafic, le marché de l'interconnexion. À cet égard, il importe de **s'assurer que l'ARCEP dispose des moyens nécessaires à l'exercice de ses missions d'étude et de surveillance**.

Recommandation n° 87

Renforcer la transparence sur la qualité des offres d'accès à internet, les risques de congestion des réseaux, les pratiques de gestion de trafic, le marché de l'interconnexion, ce qui suppose d'attribuer à l'ARCEP les moyens nécessaires à l'exercice de ses missions de surveillance et d'observation.

---

(1) *La position de la FCC a cependant évolué : selon son* Order *du 26 février 2015, la FCC se réserve la possibilité d'examiner au « cas par cas » des problèmes de neutralité provoqués par les conditions d'interconnexion.*

(2) *Conseil national du numérique,* op. cit., *p. 42.*

C. LA « LOYAUTÉ DES PLATEFORMES » : UN OBJECTIF À ATTEINDRE PAR L'ADAPTATION DU DROIT COMMUN ET LA MISE EN PLACE D'UNE RÉGULATION SPÉCIFIQUE DES GRANDES PLATEFORMES

La Commission observe que le développement exponentiel des plateformes et de leurs capacités hégémoniques constitue la nouvelle étape de la révolution numérique, faisant des grandes plateformes les nouveaux « empires industriels » de notre époque.

La notion de « loyauté des plateformes » est née de la volonté de décliner le principe de neutralité d'internet, applicable aux seuls opérateurs de communications électroniques, pour les « plateformes », autre catégorie d'intermédiaires structurants de l'économie numérique (**1**). Pour répondre aux enjeux posés par ces nouveaux acteurs, le Conseil d'État et le Conseil national du numérique ont proposé de les englober dans une catégorie juridique afin de leur appliquer un principe de « loyauté ». Cependant, la définition même des plateformes soulève un certain nombre d'interrogations de même que les obligations particulières qu'il conviendrait de leur imposer, ce qui plaide pour une clarification de cette notion (**2**). La Commission souhaite privilégier deux approches, potentiellement complémentaires : une adaptation du droit commun qui permet de dépasser les difficultés liées à la définition d'une catégorie juridique particulière et une approche par la mise en place d'une régulation spécifique qui pourrait concerner les plateformes les plus structurantes de l'économie numérique (**3**).

1. De la neutralité à la loyauté des plateformes

Alors que certains défendent l'extension du champ de la neutralité au-delà des seuls opérateurs de communications électroniques (***a***), d'autres considèrent que le principe de neutralité n'est pas transposable aux plateformes et plaident pour la consécration d'un principe de loyauté (***b***).

a. Une volonté initiale d'extension du champ de la neutralité d'internet

Le débat sur la « régulation des plateformes » est contemporain de celui sur la neutralité de l'internet. De nombreux acteurs et observateurs préconisent en effet d'**étendre le principe de neutralité au-delà des seuls opérateurs de communications électroniques** pour l'appliquer aux terminaux et aux « plateformes », avec l'idée que certaines d'entre elles, à commencer par le moteur de recherche *Google*, jouent un rôle au moins aussi important que celui des opérateurs de communications électroniques dans l'accès des internautes aux contenus et services.

Les opérateurs de communications électroniques, en particulier, insistent pour que les obligations qui seraient mises à leur charge, en vertu du principe de neutralité des réseaux, soient contrebalancées par un principe similaire de neutralité des plateformes. Cette proposition de régulation accrue des plateformes numériques est soutenue par les gouvernements français et allemand, notamment

dans une perspective de défense des acteurs européens face aux grandes plateformes essentiellement américaines.

Dans son rapport de septembre 2012 sur la neutralité de l'internet, l'ARCEP indiquait ainsi qu'« *au-delà des opérateurs et de leurs relations avec les utilisateurs,* ***le débat sur la neutralité peut concerner directement d'autres acteurs, tels que les fabricants de terminaux ou les fournisseurs de contenus et d'applications****. Certains d'entre eux,* ***particulièrement lorsqu'ils acquièrent une position dominante sur leur marché****, peuvent contribuer à favoriser certains contenus ou applications au détriment d'autres. Ainsi, le contrôle des couches logicielles d'un terminal, dont l'importance va croissante, peut permettre à certains acteurs de limiter le choix des contenus ou applications pouvant être utilisés, ou au contraire de privilégier des contenus ou applications partenaires* » (1).

Cette question n'est pas du tout traitée dans le projet de règlement européen établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté de sorte que la neutralité de l'internet ne concerne pour le moment que les opérateurs de télécommunications. Les plateformes appartiennent pour leur part à la catégorie générale et très peu régulée des services de la société de l'information. Dès lors, le cadre d'une éventuelle régulation des plateformes est intégralement à construire au plan européen.

À la demande du Gouvernement, le Conseil national du numérique a rendu en mai 2014 un avis sur la « neutralité des plateformes » (2). Le Conseil national du numérique y relevait que l'écosystème numérique n'est pas seulement déterminé par des réseaux physiques mais aussi par un ensemble de services, parmi lesquels les plateformes occupent une place centrale et « *jouent un rôle crucial pour atteindre les objectifs de la neutralité d'internet* ». Par conséquent, « *les objectifs qui ont mené à la formulation du principe de neutralité doivent conduire à en tirer les conséquences pour les plateformes numériques : il est nécessaire de s'assurer que leur développement, bien qu'utile et innovant, ne tarisse pas les dynamiques de création, d'expression et d'échange sur internet* » (3).

b. De la neutralité à la loyauté

Dans son étude annuelle 2014, le Conseil d'État estime que **le principe de neutralité ne saurait être transposable tel quel aux plateformes**. « *L'objet de ces plateformes est de* ***fournir un accès organisé, hiérarchisé ou personnalisé*** *aux contenus mis à disposition sur leur site ou auxquelles elles donnent accès. En vertu du principe de neutralité du net, un fournisseur d'accès doit traiter de la*

---

(1) ARCEP, Rapport au Parlement et au Gouvernement sur la neutralité de l'internet, *Les Actes de l'ARCEP, septembre 2012, p. 13.*

(2) Conseil national du numérique, Neutralité des plateformes, Réunir les conditions d'un environnement numérique ouvert et soutenable, *mai 2014.*

(3) Op. cit., *p. 8.*

même manière tous les contenus ; un tel traitement égalitaire ne peut être demandé à un moteur de recherche, puisque l'objet même d'un moteur de recherche est de hiérarchiser les sites internet. Les plateformes n'ont pas une responsabilité analogue à celle des gestionnaires d'infrastructures d'un réseau qui doit être universellement accessible : elles peuvent, dans le cadre de leur liberté contractuelle, exercer une sélection des services proposés » (1). Le Conseil d'État propose par conséquent de préférer à la notion de neutralité celle de **« loyauté » dans l'exercice d'organisation, de hiérarchisation et de référencement de l'information et des contenus**.

De fait, le Conseil national du numérique, dans son avis consacré à la « neutralité des plateformes », ne préconise pas d'imposer aux plateformes une obligation de neutralité analogue à celle qui incombe aux opérateurs de communications. Cependant, dans son rapport *Ambition numérique* de juin 2015, le Conseil national du numérique abandonne la notion de « neutralité des plateformes » au profit de celle de loyauté, notion plus large qui agrège une plus grande diversité d'objectifs, en particulier des objectifs de loyauté dans l'utilisation des données à caractère personnel.

2. La « loyauté des plateformes » : une notion à clarifier sans retard

La notion de « plateforme » dans l'univers numérique est une notion courante, essentiellement économique à l'origine, et associée à la théorie des marchés biface. Il s'agit d'une **notion très large** qui peut recouvrir des interprétations diverses mais au cœur de laquelle réside **le principe de l'intermédiation** entre, d'une part, un producteur ou un vendeur et, d'autre part, un utilisateur d'internet, qu'il s'agisse d'un usager ou d'un consommateur. Si l'analyse permet d'identifier des caractéristiques et des problématiques particulières propres aux grandes plateformes numériques (***a***), la définition de la notion de « plateformes » et le champ de l'obligation de « loyauté » qu'il convient de leur imposer soulèvent des interrogations et invitent à mieux les appréhender juridiquement (***b***).

a. Les plateformes numériques : une nouvelle catégorie d'acteurs qui présente des caractéristiques et problématiques spécifiques

Le monde numérique favorise l'émergence de services d'intermédiation très puissants qui proposent aux internautes une sélection et une hiérarchisation de l'offre et de l'information disponibles sur internet ainsi que des services de partage et de mise en relation (moteurs de recherche, réseaux sociaux, plateformes de partage de vidéos, magasins d'applications, etc.). Ces nouveaux acteurs, caractéristiques de l'économie numérique, remettent en cause les relations traditionnelles directes entre fournisseurs et utilisateurs finaux et soulèvent des problématiques particulières.

---

(1) Conseil d'État, op. cit., *p. 222.*

Pour M. Bruno Lasserre, président de l'Autorité de la concurrence, les plateformes créent « *des problématiques nouvelles, spécifiques, parce que nous sommes face à de nouveaux géants mondiaux (*Google, Facebook...*) qui cumulent des caractéristiques leur conférant un pouvoir de marché sans égal* » (1).

La première de ces caractéristiques est **l'effet de réseau** dont bénéficient ces services : il est d'autant plus intéressant de participer à un réseau que le nombre d'utilisateurs est important et lorsqu'un réseau a acquis une place prééminente, il devient difficile de le concurrencer, ce que l'on appelle l'effet « *winner takes all* ». L'économie numérique est ainsi marquée par des rendements d'échelle croissants : une fois consentis les investissements initiaux nécessaires à la mise en place d'un service performant, celui-ci peut être fourni à un plus grand nombre d'utilisateurs à un coût marginal presque nul.

Ces effets de réseau sont amplifiés par le fait que les plateformes numériques opèrent sur **des marchés à deux versants dits « biface », voire à plusieurs versants qualifiés de « multiface »**, c'est-à-dire qu'elles s'adressent à plusieurs types d'acteurs et se rémunèrent auprès des acteurs les plus disposés à payer. Les marchés biface favorisent de puissants effets de réseau croisés : plus il y a d'utilisateurs sur un versant du marché, plus la plateforme peut valoriser le service ou le produit qu'elle propose sur l'autre versant. Les plateformes de paiement par carte bancaire, les médias financés par la publicité ou les opérateurs de télécommunications constituent également des marchés biface. Ces modèles ne sont donc pas nouveaux mais leurs effets sont amplifiés dans l'univers numérique en raison d'une empreinte géographique sans équivalent et de la prévalence d'un modèle de gratuité apparente, par exemple celui fondé sur la collecte et le traitement de données à caractère personnel. Comme le souligne M. Bruno Lasserre, « *c'est un modèle d'une très grande force. Ainsi, le moteur de recherche* Google *donne l'illusion d'une utilisation gratuite à l'internaute (qui « paye » en réalité en transmettant de multiples données sur son profil, son comportement, ses préférences, véritable « carburant » de ce type d'entreprise) mais il ne faut pas oublier l'autre face du marché, celle des annonceurs, qui achètent des mots-clés* » (2).

Par ailleurs, les plateformes numériques se caractérisent souvent par **une intégration verticale** : « *ces acteurs se diversifient pour aller chercher de la valeur en aval, tel* Google *dans les moyens de paiement, les contenus avec* YouTube, *les télécoms avec son projet d'opérateur mobile virtuel aux États-Unis… Ils ne se contentent plus d'être des acteurs de la mise en relation mais deviennent eux-mêmes des marchands. Cette combinaison peut construire de véritables forteresses* » (3). Comme le souligne le Conseil national du numérique,

---

(1) Bruno Lasserre, entretien donné à l'Opinion, *16 mars 2015.*

(2) Ibid.

(3) Ibid.

« *plusieurs plateformes ont adopté des modèles de développement basés sur la constitution de véritables écosystèmes dont elles occupent le centre* » [(1)].

On avance souvent que la concurrence est « à un click » et que l'innovation rapide et constante, qui est également une spécificité de l'économie numérique, est susceptible de remettre en cause les positions acquises. Il est vrai que *Microsoft* occupait au début des années 2000 la position qu'exerce aujourd'hui *Google* avec son moteur de recherche. Cependant, la tendance de ces acteurs dominants à étendre constamment leurs activités à de nouveaux services et à racheter les acteurs émergents susceptibles de leur faire concurrence pourrait rendre plus difficile à l'avenir la remise en cause de ces positions.

Ces plateformes sont ainsi **devenues des intermédiaires quasi-incontournables** pour les internautes comme pour les entreprises qui fournissent des services et des contenus sur internet. Elles leur offrent des **services innovants d'une utilité indéniable** : facteurs de transparence sur la nature et l'étendue de l'offre, elles permettent aux internautes d'arbitrer, d'agir, de s'informer, avant de faire un choix mais aussi à l'offreur référencé de bénéficier d'une exposition large, souvent mondiale.

Si elles permettent aux entreprises référencées de toucher un large public et de profiter d'effets de réseaux importants, certaines plateformes numériques peuvent abuser de leur pouvoir économique pour **imposer des conditions contractuelles significativement déséquilibrées à leurs partenaires commerciaux.**

Lorsque les plateformes sont verticalement intégrées, elles peuvent par ailleurs **restreindre la concurrence en intervenant notamment sur la visibilité des offres de leurs concurrents, au profit des leurs**.

Ce positionnement leur permet également de **capter une partie non négligeable de la valeur** issue des services et des contenus créés par des tiers, et de placer leurs partenaires commerciaux dans une situation de **dépendance économique**.

En ce qui concerne les internautes, les plateformes leur proposent des services et interfaces très utiles et largement plébiscités mais certains de leurs comportements peuvent aussi leur être préjudiciables.

Beaucoup de plateformes, par leur rôle de **prescripteurs**, façonnent et déterminent nos conditions d'accès aux informations. Elles ne permettent pas toujours de déterminer facilement si ce qui est présenté relève de la publicité, d'une sélection algorithmique générique, d'une adaptation personnalisée ou d'une préférence pour l'offre de la plateforme hôte.

---

(1) Avis n° 2014-2 du Conseil national du numérique relatif à la neutralité des plateformes.

Dans son étude annuelle 2014, le Conseil d'État souligne **les problèmes spécifiques que peuvent poser les algorithmes** qui sont « *au cœur du rôle d'intermédiation joué par les plateformes* » : risque d'enfermement de l'internaute dans une « personnalisation » dont il n'est pas maître ; confiance abusive dans les résultats d'algorithmes supposés objectifs et infaillibles ; apparition de problèmes nouveaux d'équité posés par l'exploitation de plus en plus fine des données personnelles. Pour le Conseil d'État, c'est d'ailleurs l'utilisation qu'elles font des algorithmes qui justifie que soient imposées aux plateformes des obligations spécifiques que le droit actuel ne prévoit pas, ou ne prévoit que de manière incomplète ou insuffisante [(1)]. Les mécanismes de sélection opérés par les plateformes peuvent donc à terme se traduire par une réduction de la qualité et de la diversité du choix global et des conditions d'information.

Par ailleurs, en ce qui concerne l'accès à l'information, il convient de rappeler que **ces plateformes définissent leurs propres règles relatives aux contenus autorisés** (standards de la communauté *Facebook*, règlement de la communauté *Youtube*, conditions d'utilisation de *Google*, chartes…) et se donnent le droit de retirer les contenus qui ne correspondent pas à ces règles. Si cette situation est conforme à leur liberté d'entreprendre et à leur liberté contractuelle, ces acteurs jouent *de facto* un rôle majeur dans l'accès à l'information et l'exercice de la liberté d'expression. À titre d'exemple *Facebook*, au nom de la protection de l'enfance, « *impose des limites à l'affichage de certaines parties du corps* ». Un artiste danois, Frode Steinicke, a ainsi été exclu du réseau social pour avoir mis sur son profil le tableau *L'Origine du monde* de Gustave Courbet de 1886, représentant un sexe féminin, car ayant contrevenu au règlement de ce réseau social. La presse a rapporté que des photos de « boobies », espèce d'oiseaux australienne dont le nom signifie « seins » en anglais familier, mises en ligne par l'office du tourisme d'une île australienne avaient également été censurées par le réseau social. De nombreux observateurs s'inquiètent ainsi de l'importance prise par les grands opérateurs, devenus quasiment des régulateurs et mettent en garde contre une sorte de **privatisation du contrôle de la liberté d'expression.**

Les enjeux économiques posés par les plateformes peuvent donc aller de pair avec des **enjeux de pluralisme, de liberté d'expression et d'accès à l'information**.

Les grandes plateformes, d'envergure mondiale pour la plupart, soulèvent également des interrogations quant à leur capacité à respecter les règles de protection de la vie privée, les règles fiscales et les différents droits nationaux, en particulier les mécanismes visant à favoriser le financement de la création et la diversité culturelle.

Enfin, on peut noter que la plupart des plateformes sont susceptibles de bénéficier par ailleurs du statut d'hébergeur et sont à ce titre soumises à une responsabilité limitée à l'égard des contenus mis en ligne par des tiers, statut qui

---

(1) Conseil d'État, op. cit., *p. 223.*

favorise déjà une forme de « neutralité » de ces acteurs. Il n'est donc pas à exclure que certains cherchent à intégrer à la notion de « loyauté » de plus grandes responsabilités de ces acteurs à l'égard des contenus illégaux.

b. La « loyauté des plateformes » : une notion majeure, à mieux appréhender juridiquement

On le voit, les plateformes soulèvent un grand nombre de problématiques et plusieurs objectifs s'entrecroisent lorsqu'il est question de les « réguler ». **En fonction de l'objectif poursuivi, la définition de la plateforme peut donc varier de même que les obligations que l'on souhaite rattacher à la notion de « loyauté »**. Le Conseil d'État et le Conseil national du numérique ont récemment proposé de créer une catégorie juridique des « plateformes » qui se verrait appliquer une obligation de « loyauté ». Les rapports de ces deux institutions ne se rejoignent ni sur la définition des plateformes ni sur celle de la loyauté de sorte que ces propositions suscitent encore de nombreuses interrogations.

i. La loyauté des plateformes selon le Conseil d'État

Le Conseil d'État propose de définir les plateformes **par rapport aux éditeurs et aux hébergeurs et de créer, dans la directive « commerce électronique » de 2000, une nouvelle catégorie juridique qui se verrait imposer une obligation de « loyauté »** (voir l'encadré ci-après).

Par rapport aux hébergeurs purement passifs et aux éditeurs, caractérisés par leur liberté éditoriale, il est proposé de viser les acteurs qui, sans avoir un véritable rôle éditorial, utilisent des services de référencement ou de classement. Le Conseil d'État propose donc de qualifier de plateformes « *les services de référencement ou de classement de contenus, biens ou services édités ou fournis par des tiers et partagés sur le site de la plateforme* ». Selon le Conseil d'État, « *cette définition cherche à capturer ce qui caractérise la plateforme, c'est-à-dire son rôle d'intermédiaire actif dans l'accès à des contenus, des biens ou des services qui ne sont pas produits par elle* » [(1)]. Le Conseil d'État en fournit une première liste : moteurs de recherche, réseaux sociaux, sites de partage de contenus (vidéos, musique, photos, documents, etc.), places de marché, magasins d'applications, agrégateurs de contenus ou comparateurs de prix.

L'obligation de loyauté selon le Conseil d'État

En ce qui concerne la loyauté, pour le Conseil, elle « *consiste à assurer de bonne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs. La plateforme doit avoir le choix des critères présidant à son classement ; mais ces critères doivent être pertinents par rapport à l'objectif de meilleur service rendu à l'utilisateur et ne peuvent par exemple être liés au fait que la plateforme favorise ses propres entités au détriment de services concurrents ou a passé des*

(1) Conseil d'État, op. cit., *pp. 272-273.*

accords de partenariat dont l'utilisateur n'aurait pas connaissance ». Le Conseil décline **plusieurs obligations** des plateformes découlant du principe de loyauté :

– pertinence des critères de classement et de référencement mis en œuvre par la plateforme au regard de l'objectif de meilleur service rendu à l'utilisateur ;

– information sur les critères de classement et de référencement ;

- définition des critères de retrait de contenus licites en termes clairs, accessibles à tous et non discriminatoires ;

- obligation de mettre l'utilisateur ayant mis en ligne un contenu en mesure de faire valoir ses observations en cas de retrait de celui-ci ;

– obligation de notification préalable, avec un délai de réponse raisonnable, des changements dans la politique de contenus ou de l'algorithme susceptibles d'affecter le référencement ou le classement.

Le contrôle et la sanction des manquements à l'obligation de loyauté relèveraient de **différentes autorités**, « *en raison de la diversité des utilisateurs des plateformes* ». *« Lorsque ces manquements affectent les consommateurs, ils pourraient être appréhendés et punis par la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF). Lorsqu'ils concernent des professionnels utilisateurs de la plateforme, ils sont susceptibles d'entrer dans les compétences de l'Autorité de la concurrence, s'ils sont constitutifs d'abus de position de dominante, ou dans celles de l'ARCEP, s'ils sont relatifs à un différend avec un FAI sur des conditions techniques et tarifaires d'interconnexion revêtant un caractère discriminatoire ou manquant de transparence. Enfin, le juge judiciaire pourrait toujours être saisi sur le terrain de la responsabilité ou dans le cadre des actions juridictionnelles spécifiques prévues par le droit de la consommation* ».

Source : Conseil d'État, op. cit., pp. 273-281.

La Commission ne souscrit pas à la proposition du Conseil d'État d'appréhender la notion de plateforme par opposition aux hébergeurs et aux éditeurs pour des raisons qui sont précisément exposées dans le II du présent rapport [(1)]. La Commission identifie un risque de brouillage des catégories et objectifs de l'article 6 de la LCEN, qui ne constituent pas le bon vecteur pour appréhender les plateformes.

Ce faisant, la définition proposée par le Conseil d'État est à la fois trop étroite et trop large.

Comme le précise le Conseil d'État, **la catégorie qu'il propose de créer ne couvre pas les éditeurs, c'est-à-dire les acteurs ayant une responsabilité directe dans la production ou la sélection des contenus mis en ligne** (*Netflix*, *Deezer*, *Spotify*, *Amazon*, *ITunes*…) qui peuvent pourtant constituer des plateformes incontournables auxquelles il pourrait être pertinent de fixer un objectif de loyauté.

Par ailleurs, **la catégorie juridique proposée par le Conseil d'État ne cible pas les acteurs en position dominante**. À cet égard, la Commission estime

(1) Voir supra, *le* a *du 1 du C du II.*

que certaines des obligations que le Conseil d'État propose d'imposer aux plateformes au titre de la loyauté, en particulier l'obligation de notification préalable en cas de changement de la politique de contenus ou de l'algorithme ou l'obligation de mettre l'utilisateur ayant mis en ligne un contenu en mesure de faire valoir ses observations en cas de retrait de celui-ci, risquent d'être **disproportionnées pour de petites plateformes et pourraient par conséquent nuire à la liberté d'entreprendre et d'innovation**. Mettre à la charge de toutes les plateformes, quelle que soit leur taille, les mêmes obligations alors que seules les grandes sont en mesure de les respecter risque de renforcer les barrières à l'entrée et de favoriser les acteurs en position dominante.

ii. La loyauté des plateformes selon le Conseil national du numérique

L'avis du Conseil national du numérique consacré à la neutralité des plateformes ne proposait pas la création d'une catégorie juridique spécifique et formulait des recommandations centrées sur l'adaptation du droit commun.

En revanche, le rapport remis au Premier Ministre par le Conseil national du numérique en juin 2015 **reprend l'idée du Conseil d'État de créer une catégorie juridique des plateformes** (sans reprendre l'idée d'en faire une troisième catégorie entre les hébergeurs et les éditeurs au sens de la LCEN, et ce afin de ne pas modifier le régime de responsabilité limitée auquel elles sont aujourd'hui soumises) **pour les soumettre à un principe de loyauté** (voir l'encadré ci-après). Alors que son rapport sur la neutralité des plateformes privilégiait une approche par l'adaptation du droit commun, le Conseil part cette fois du constat que le droit existant et le droit commun souffrent d'ineffectivité et d'impuissance face aux problématiques spécifiques aux plateformes. La consécration du principe de loyauté vise par conséquent « *à donner un nouveau souffle aux dispositions du droit positif en particulier le droit de la concurrence, le droit commercial, le droit de la consommation et le droit de la protection des données, en apportant un nouveau fondement juridique permettant une approche décloisonnée* » (1).

Les définitions proposées par le Conseil national du numérique et le Conseil d'État tant pour les plateformes que pour la loyauté ne se rejoignent pas.

Pour le Conseil national du numérique, une plateforme « *pourrait être définie comme un service occupant une fonction d'intermédiaire dans l'accès aux informations, contenus, services ou biens,* ***le plus souvent*** *édités ou fournis par des tiers. Au-delà de sa seule interface technique, elle organise et hiérarchise ces contenus en vue de leur présentation et leur mise en relation aux utilisateurs finaux. À cette caractéristique commune s'ajoute* ***parfois*** *une dimension écosystémique caractérisée par des interrelations entre services convergents* » (2).

---

(1) Conseil national du numérique, Ambition numérique, op. cit., *p. 59.*

(2) Ibid.

Cette définition apparaît particulièrement large puisqu'elle semble à première vue pouvoir inclure l'ensemble des fournisseurs de contenus et services sur internet.

Le Conseil national du numérique propose ensuite de cibler certaines obligations sur une sous-catégorie des plateformes : les **plateformes « *dotées de la plus forte capacité de nuisance* »**. Ces dernières seraient définies par « *le recours à un faisceau d'indices* » (audience ; adoption massive par les utilisateurs du service ou du groupe de services convergents ; non-respect avéré et récurrent des règles de protection des données ; pouvoir de nuire à l'innovation et d'évincer un acteur) [(1)].

Le principe de loyauté selon le Conseil national du numérique

S'agissant du principe de loyauté, pour le Conseil, il vise à « obliger les acteurs économiques à assurer **de bonne foi** les services qu'ils proposent sans chercher à les détourner à des fins contradictoires à l'intérêt de leurs utilisateurs, qu'ils soient particuliers ou professionnels ».

Pour la plateforme, ce principe implique premièrement et d'une manière générale la **transparence** de son comportement, condition pour s'assurer de la conformité entre la promesse affichée du service et les pratiques réelles.

Dans les relations avec les individus, le principe vise également les modes de collecte, de traitement des données et de restitution de l'information, notamment en ce qui concerne les algorithmes de personnalisation. Il implique ensuite le respect d'un **principe général de non-discrimination** (ex : proposer des services à un prix supérieur aux utilisateurs d'ordinateurs de la marque Apple, supposés bénéficier de revenus plus élevés). Il s'applique en particulier au filtrage des formes d'expressions et de contenus partagés des individus, hors contenus condamnables par la loi.

Le Conseil national distingue deux dimensions du principe de loyauté :

– **dans les relations de la plateforme avec ses utilisateurs**, le principe de loyauté s'appliquerait à toutes les plateformes, à l'instar des règles de protection des consommateurs qui imposent un devoir général de conseil et d'information à tous les professionnels vis-à-vis des particuliers ;

– **dans les relations de la plateforme avec ses utilisateurs professionnels**, l'application du principe doit se concentrer, à l'instar des règles communes de la régulation économique, sur les pratiques qui pénalisent le plus l'innovation. Par conséquent, il **se concentre sur les acteurs dotés de la plus forte capacité de nuisance**.

Dans sa partie consacrée à la « loyauté des plateformes », le Conseil décline ensuite toute une série d'obligations qui découleraient du principe de loyauté, lequel est présenté comme le prolongement de l'autodétermination informationnelle : édicter des conditions générales d'utilisation (CGU) lisibles en matière d'exploitation des données personnelles ; assurer l'application effective de l'« opt-in », rendre transparente pour l'utilisateur l'audience de diffusion des messages et contenus qu'il poste ; introduire un droit à la transparence et à la conformité aux engagements de la plateforme des algorithmes destinés à la personnalisation, au classement ou au référencement ; obtenir des garanties de la part des acteurs contre l'utilisation discriminante des données dans les politiques de prix ; demander aux grandes plateformes de respecter des engagements de pluralisme de l'information délivrée et d'offrir la possibilité de désactiver la personnalisation des résultats de leur service ; instaurer une obligation d'information préalable dans des délais raisonnables en cas de modifications majeures, telles que des changements de politiques tarifaires, de

(1) Ibid, *p. 61.*

contenus, d'accès aux API ou de changements substantiels des critères de classement par algorithmes ; appliquer un principe de non-discrimination dans le référencement, sauf en cas de considérations légitimes, vérifiables par des tiers et conformes à l'intérêt des internautes ; ouvrir et maintenir des passerelles entre grands écosystèmes concurrents ; mettre en place des principes adaptés à l'économie numérique qui s'inspirent du droit des pratiques restrictives de la concurrence ; adapter le design institutionnel...

Pour « rendre le principe de loyauté effectif », le CNNum estime qu'un contrôle doit être exercé par les autorités de régulation, « notamment la CNIL, l'ARCEP, le CSA, l'Autorité de la concurrence, la DGCCRF, la Commission des clauses abusives, la Commission d'examen des pratiques commerciales, le Défenseur des droits, etc. » La répartition des compétences n'est donc pas clairement établie.

Il est proposé d'appuyer l'action de ces autorités par **une agence européenne de notation de la loyauté** fondée sur un réseau ouvert de contributeurs et un corps d'experts en algorithmes mobilisable sur demande d'une autorité de régulation.

Source : Conseil national du numérique, op. cit., pp. 60-76.

Le Conseil national du numérique fait donc de la loyauté un concept extrêmement large. Et l'on peut d'ailleurs s'interroger sur la pertinence de limiter certaines de ces obligations aux seules plateformes. Certaines sont d'ailleurs prévues par le projet de règlement sur la protection des données et ont vocation à s'appliquer à tous les acteurs qui utilisent des données à caractère personnel.

Ces propositions ont été critiquées notamment **pour le caractère multiforme voire flou tant des concepts de plateformes et que des obligations qu'il est proposé de leur imposer**.

Certaines obligations, notamment celles relatives à la mise en visibilité des critères généraux et des principes directeurs de leurs algorithmes, suscitent de nombreuses réserves. En effet, si les critères des algorithmes sont rendus publics, il est certain que les opérateurs de sites chercheront à s'adapter afin d'améliorer leur référencement au risque de remettre en cause la pertinence de tout algorithme. En outre, lors de son audition par la Commission le 7 juillet 2015, M. Bruno Lasserre, président de l'Autorité de la concurrence a estimé que « *la transparence s'arrête là où commence le risque pour l'innovation et pour la protection du secret des affaires ; l'innovation suppose que tout ne soit pas rendu public. Je m'interroge enfin sur la capacité des consommateurs, une fois qu'ils prendraient connaissance de l'algorithme, à se protéger contre toutes les manipulations indésirables de celui-ci. Je suis donc sceptique quant à l'utilité d'une communication intégrale des algorithmes et préoccupé par les risques qu'elle pourrait induire* ».

Ces propositions sont également contestées tant par ceux qui privilégient une approche par le droit commun que par ceux qui appellent à une véritable régulation *ex ante* des grandes plateformes et en particulier de *Google* (1).

---

(1) Voir en particulier, « Une agence de notation des géants du net, une fausse bonne idée ? », La Tribune, *26 juin 2015.*

On peut par ailleurs regretter que la polarisation du débat autour de la notion de « loyauté des plateformes » ait quelque peu fait perdre de vue **la question des terminaux**, qui n'entrent pas dans la catégorie, et qui constituent pourtant un enjeu crucial pour la garantie d'un internet ouvert.

3. Deux grandes approches possibles pour appréhender les plateformes

La Commission identifie deux grandes approches pour appréhender la problématique des plateformes à l'ère numérique : une approche par l'adaptation du droit commun et une approche par la mise en place d'une régulation *ad hoc* des grandes plateformes numériques. Ces deux approches ne sont d'ailleurs pas exclusives l'une de l'autre. **Une majorité des membres de la Commission estime en effet qu'il est nécessaire de rendre plus effectifs et d'adapter les outils du droit commun existant (*a*) tout en envisageant la mise en place d'une régulation *ad hoc* des grandes plateformes structurantes de l'économie numérique (*b*)**. Les deux approches peuvent être envisagées simultanément ou successivement, au cas où l'adaptation du droit commun s'avérerait insuffisante.

a. Une approche par l'adaptation du droit commun

Comme l'indique le Conseil national du numérique dans son avis sur la neutralité des plateformes, les plateformes numériques ne sont pas des espaces de non-droit et bon nombre des difficultés qu'elles soulèvent « *peuvent être traitées en exploitant au mieux les droits existants : consommation, commercial, concurrence, données, etc.* ».

L'avantage de cette approche est qu'elle est technologiquement plus neutre et qu'elle permet une approche transversale, la numérisation concernant tous les champs de l'économie. Par ailleurs, elle n'oblige pas à définir une catégorie juridique des plateformes avec les difficultés et l'insécurité juridique qu'une telle définition entraîne ni à définir une notion potentiellement très large et trop floue de « loyauté ».

Dans un article « *Réguler les plateformes : une fausse bonne idée* » publié dans *L'Opinion* le 23 avril 2015, MM. Winston Maxwell, avocat membre de la Commission, et Thierry Pénard, professeur d'économie, soulignent également qu'« ***il existe déjà un arsenal permettant de répondre aux pratiques éventuellement abusives qui inquiètent les pouvoirs publics :*** *l'abus de position dominante est sanctionné par le code de commerce. Les pratiques déloyales dans le commerce sont elles aussi sanctionnées par le même code, et ces dispositions ont été mises en œuvre contre* Kelkoo. *Le code de la consommation impose des obligations de transparence et de loyauté à l'égard des consommateurs, et ces dispositions ont récemment été précisées dans le cadre des relations entre les réseaux sociaux et leurs utilisateurs (décision de la Commission de clauses abusives de novembre 2014). La CNIL veille au respect des données personnelles, et la législation dans ce domaine sera bientôt renforcée grâce à l'adoption d'un règlement européen.* ***En réalité, chaque mal possède déjà son remède*** ».

Cette approche n'exclut pas des adaptations du droit commun aux nouveaux défis posés par les plateformes. Dans son rapport sur la neutralité des plateformes, le Conseil national du numérique préconisait d'adapter le cadre et les modalités du droit de la concurrence, du droit commercial, du droit de la consommation et du droit de la protection des données à caractère personnel aux « nouveaux espaces de droit que sont les plateformes ».

La Commission se propose d'évoquer, sans prétendre à l'exhaustivité, quelques pistes d'adaptation du droit commun permettant d'apporter de premières réponses aux problématiques soulevées par les plateformes.

i. Le droit de la concurrence

Le droit de la concurrence, qui s'applique de plein droit à l'économie numérique, est concerné au premier chef. Le droit de l'Union européenne (articles 101 et 102 du Traité sur le fonctionnement de l'Union européenne) et la loi française (articles L. 4201-1 et L. 420-2 du code de commerce) énoncent des règles générales de concurrence applicables à l'ensemble des activités de production, de distribution et de services. Les abus de position dominante sont interdits de même que les ententes ayant pour objet ou pour effet de fausser le jeu de la concurrence.

Lors de son audition par la Commission, le 7 juillet 2015, M. Bruno Lasserre, président de l'Autorité de la concurrence, a mis en avant **les atouts du droit de la concurrence sur la régulation sectorielle** :

Premièrement, « *l'avantage du droit de la concurrence, c'est qu'il* ***s'applique à toute activité économique*** *– production de biens, offre de services ou activité de distribution –,* ***sans que nous ayons besoin de la qualifier****. Nous pouvons intervenir de deux manières : soit parce qu'il existe une dominance – notion dont nous nous sommes servis face à des acteurs tels que* Google *–, soit parce qu'on se trouve dans le cadre de relations contractuelles, comme dans le cas des plateformes de réservation hôtelière et des opérateurs référencés. Dès lors qu'il y a contrat – notamment de distribution –, le droit de la concurrence permet de vérifier qu'il est exempt d'obstacles concurrentiels* ».

Deuxièmement, « *le droit de la concurrence tire sa force de* ***son caractère mondial****, davantage encore dans ce domaine où les acteurs se jouent des territoires. Il est appliqué dans 130 pays dans le monde. Au sein de l'ICN (*International competition network*), les autorités de la concurrence essaient d'unifier les concepts et de promouvoir les bonnes pratiques. Vis-à-vis des opérateurs américains qui le connaissent et le craignent, ce droit est une force de dissuasion plus efficace que les multiples régulations nationales avec lesquelles ils doivent jouer. Ce droit mondial est néanmoins appliqué par des autorités régionales ou nationales qui peuvent d'autant plus agir que les comportements en cause produisent des effets à leur échelle* ».

Troisièmement, « *le droit de la concurrence n'est pas seulement punitif :* ***les entreprises peuvent prendre des engagements par lesquels elles remédient elles-mêmes à certains dysfonctionnements****. Il me semble important que certains abus soient corrigés à l'intérieur du marché et non pas forcément sur intervention législative ou régulatrice. C'est ainsi que* Booking, Expedia *et* HRS *se sont engagées à lever la plupart des clauses de parité tarifaire qui interdisent une véritable mise en compétition de ces plateformes de réservation hôtelières. Comment fonctionnent ces clauses ? Si un hôtel réserve à* Booking *douze nuitées au prix de 100 euros la chambre, il ne peut offrir de meilleures conditions – en disponibilité ou en tarif – aux autres plateformes. Il ne peut pas non plus pratiquer un prix différent à ses clients directs. Les engagements signés pour lever ces contraintes sont gagnants-gagnants : ils respectent le modèle économique des plateformes, et donc l'incitation à investir et à innover, tout en rétablissant plus de liberté de négociation. Les hôtels pourront désormais mettre les plateformes en concurrence. En outre, cette méthode permet d'aller plus vite : négociés en avril, les engagements sont entrés en vigueur le 1er juillet, et il n'y a pas de risques de contentieux puisqu'ils ont été signés par les entreprises elles-mêmes. Ce sont des remèdes très définis, très prescriptifs.* Booking *s'est engagé à abandonner les principales clauses de parité tarifaire ou de disponibilité, mais aussi à ne pas prendre d'autres mesures qui produiraient le même effet : déréférencement, augmentation des commissions, dégradation de l'exposition publique d'hôtels qui réduiraient de manière agressive le prix de leurs chambres sur d'autres plateformes ou en ventes directes* ».

Certains appellent néanmoins à des adaptations de ce droit à l'ère numérique afin qu'il puisse être davantage mobilisé à l'égard des plateformes. Dans son avis sur la neutralité des plateformes, le Conseil national du numérique préconise en particulier **une adaptation des concepts de position dominante ou d'infrastructure essentielle** pour « *prendre en compte les nouvelles formes de domination dans l'accès des tiers à leurs clients grâce à des stratégies d'intermédiation, la constitution de silos, la création d'un écosystème de référence pour les partenaires, l'accumulation de données ou encore la consultation d'informations sur l'état du marché et les préférences des utilisateurs non duplicables* ».

Lors de son audition par la Commission, M. Bruno Lasserre a défendu la robustesse et la plasticité des notions d'infrastructure essentielle [(1)] et de position dominante à l'ère numérique et mis en garde contre une modification des standards du droit de la concurrence.

---

(1) Une infrastructure est essentielle lorsque (i) l'infrastructure est possédée par une entreprise qui détient un monopole (ou une position dominante) ; (ii) l'accès à l'infrastructure est strictement nécessaire (ou indispensable) pour exercer une activité concurrente sur un marché amont, aval ou complémentaire de celui sur lequel le détenteur de l'infrastructure détient un monopole (ou une position dominante) ; (iii) l'infrastructure ne peut être reproduite dans des conditions économiques raisonnables par les concurrents de l'entreprise qui la gère ; (iv) l'accès à cette infrastructure est refusé ou autorisé dans des conditions restrictives injustifiées ; (v) l'accès à l'infrastructure est possible.

S'agissant de la notion de position dominante, il a rappelé qu'elle était suffisamment claire et souple et que les spécificités de l'économie numérique ne remettaient aucunement en cause sa pertinence. « *Cette notion très souple a été rappelée, dès 1979, par la jurisprudence Hoffmann-La Roche de la Cour de justice des Communautés européennes : la détention d'une position dominante est liée à la possibilité, pour une entreprise, d'adopter des "* comportements indépendants dans une mesure appréciable vis-à-vis de ses concurrents, de ses clients et in fine des consommateurs *". D'aucuns prétendent que cette notion aurait mal vieilli et qu'elle mériterait un* aggiornamento. *Pour ma part, je pense qu'elle est claire et suffisamment plastique pour s'adapter à des configurations très différentes, notamment quand il s'agit d'évaluer le pouvoir de marché des nouveaux acteurs du numérique. C'est ainsi que l'Autorité de la concurrence française a pu l'utiliser pour se prononcer sur le rachat d'*AdWords *par* Google, *par exemple* ».

S'agissant de la théorie des infrastructures essentielles, il a souligné que la caractérisation d'une infrastructure essentielle n'était pas un préalable nécessaire à une intervention efficace, contrairement à ce qui est souvent affirmé. La théorie est en effet applicable à des hypothèses d'actifs immatériels [(1)] : elle peut donc permettre d'appréhender des ressources-clés qui ne sont pas des infrastructures physiques.

Par ailleurs, comme l'a rappelé M. Bruno Lasserre, il existe également une pratique décisionnelle constante de l'Autorité reposant sur **l'identification de comportements discriminatoires, qualification qui permet en pratique d'aboutir souvent aux mêmes résultats que le détour par la théorie des infrastructurelles essentielles**. Une autorité de concurrence, par le biais de la condamnation des discriminations abusives, peut notamment remédier à une situation dans laquelle un opérateur dominant impose ses propres applications ou ses propres services au détriment d'opérateurs concurrents, en mobilisant la sanction et les pouvoirs qui lui sont conférés (voir l'encadré ci-après).

Exemples d'application du droit de la concurrence à des plateformes

Dans l'affaire *NavX* (2010), qui porte précisément sur la question de l'accès à une « plateforme », l'Autorité a enjoint à *Google* de modifier sa politique de contenus *AdWords* en clarifiant le contenu des interdictions ainsi que les procédures de suspension qui découlent de leur violation. L'Autorité a qualifié le comportement de *Google* de discriminatoire et a fixé, de manière concrète et opérationnelle, des principes qui sont proches, dans leur contenu, de ceux que le Conseil d'État englobe dans la notion de « loyauté » (précision sur le champ des interdictions fixées par la politique de contenus *AdWords*, y compris leur modification avec un préavis de trois mois ; précision sur la procédure mise en œuvre en cas de contrariété avec la politique de contenus ; préavis obligatoire avant suspension du compte). L'Autorité de la concurrence a, dans cette affaire,

(1) Il existe un précédent d'application, avec succès, par le Conseil de la concurrence de la théorie des infrastructures essentielles à une nomenclature protégée au titre du droit d'auteur et du droit sui generis *des bases de données.* http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=149&id_article=423.

utilisé une procédure d'urgence l'ayant conduite à rendre sa décision en moins de quatre mois.

Le 21 avril 2015, le site *Booking.com* a conclu un accord avec l'Autorité de la concurrence pour mettre un terme à certaines de ses pratiques jugées anticoncurrentielles dans ses contrats avec les hôtels.

Le 31 janvier 2012, *Google* a été condamné pour abus de position dominante dans le cadre de *Google Maps*.

Par ailleurs, le comportement reproché par la Commission européenne dans le dossier *Google*, dans son volet relatif au service de comparateur de prix *Google Shopping*, est également un comportement discriminatoire, consistant plus précisément, pour *Google*, à réserver un traitement plus favorable, sur les pages de résultats du moteur de recherche naturelle, à ses propres services de comparateurs de prix par rapport aux services de comparateurs de prix concurrents, en termes de positionnement et d'affichage. En l'espèce, **la difficulté rencontrée par la Commission n'est pas tant celle de la qualification de la pratique que celle de la détermination du remède à appliquer** : faut-il interdire à *Google* d'afficher ses propres résultats de comparateurs de prix ? Faut-il un principe d'équivalence stricte entre ses résultats et ceux de ses concurrents ? Jusqu'à quel point *Google* est-il autorisé à monétiser la mise à disposition d'un espace réservé à ses concurrents ? Si l'adaptation de la notion de position dominante aboutirait éventuellement à caractériser plus facilement un abus, elle ne règlerait pas la question de la détermination du remède adapté et proportionné à l'abus constaté.

S'agissant de l'appréhension des marchés biface et des effets de réseau croisés, on peut noter qu'il existe une pratique décisionnelle constante de l'Autorité consistant à sanctionner l'utilisation croisée de données (à savoir le fait d'utiliser les données commerciales déjà détenues sur un marché pour se développer sur un autre marché) lorsque la détention de ces données constitue un avantage non réplicable et que leur utilisation présente un réel risque d'éviction [(1)].

Le président de l'Autorité de la concurrence a néanmoins suggéré **certaines adaptations des modalités d'intervention du droit de la concurrence**.

La procédure pour abus de position dominante engagée à l'encontre de *Google*, critiquée en particulier pour sa lenteur dans un secteur caractérisé par la rapidité de ses évolutions, est souvent présentée comme symptomatique de l'inadaptation du droit de la concurrence.

À cet égard, M. Bruno Lasserre a regretté la **sous-utilisation** par les autorités de concurrence en Europe de la possibilité d'imposer **des mesures d'urgence unilatérales**, qui peuvent intervenir dans un délai de trois à quatre mois sans attendre l'instruction au fond sur la base d'un examen *prima facie* du cas et de l'identification de risques immédiats pour la concurrence. « *La force*

---

(1) Si l'utilisation croisée des bases de clientèle est particulièrement problématique lorsqu'elle est le fait d'une entreprise détentrice d'un monopole historique, l'Autorité a souligné, dans le cadre de son enquête sectorielle de 2010 sur les pratiques dites de « cross-selling » (http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=367&id_article=1412), qu'une telle pratique était également susceptible de dégénérer en abus hors de l'hypothèse restreinte d'un monopole, dès lors que les données en cause sont difficilement réplicables et leur utilisation présente un risque réel d'éviction (http://www.autoritedelaconcurrence.fr/pdf/avis/10a13.pdf; voir paragraphe 26).

*d'*Uber *et des autres, c'est leur rapidité (…) ils peuvent créer une situation de fait accompli sur laquelle il sera très difficile de revenir. Les autorités de la concurrence doivent s'adapter et utiliser les moyens d'urgences dont elles disposent, c'est-à-dire les mesures conservatoires. L'Autorité de la concurrence française est quasiment la seule en Europe à en faire usage. (…) L'investigation européenne sur* Google *montre que si des mesures conservatoires avaient été imposées d'emblée, le rapport de force et la maîtrise du temps auraient pu être envisagés de manière différente. J'appelle à un* aggiornamento *qui ne concernerait pas tant les concepts et les standards que les modes d'intervention (…). Même si la solution de fond est satisfaisante, elle arrivera trop tard pour corriger une situation qui risque d'être devenue irréversible. Le règlement 1/2003/CE cite les mesures conservatoires comme l'un des outils dont doivent disposer les autorités de la concurrence européennes. Pourtant, il n'y a qu'en France – et de façon moins nette en Espagne – que cet outil est utilisé. Dans toute son histoire, la Commission européenne ne s'en est servie qu'une seule fois* ».

Par ailleurs, le président de l'Autorité de la concurrence a également appelé à s'interroger sur **l'adaptation des critères d'examen des opérations de concentration** actuellement définis en fonction du seul chiffre d'affaires. Ce critère, dont la clarté et la simplicité présente l'avantage d'offrir aux acteurs une importante sécurité juridique, ne permet pas d'appréhender des entreprises disposant d'un potentiel de croissance non encore monétisé assis sur la collecte et le traitement d'un grand nombre de données à caractère personnel et une base d'utilisateurs importante susceptibles d'engendrer d'importants effets de réseau.

Lors d'un colloque consacré à régulation des plateformes numériques [(1)], M. Marc Lebourges, représentant d'*Orange* et président du groupe de travail « Competition Policy » de l'ETNO (*European Telecommunications Network Operators*) a estimé, à la lumière de la décision de la Commission européenne d'autoriser sans condition le rachat de *What's App* par *Facebook*, que « *pour des plateformes globales opérant sur des marchés biface avec des volumes d'activité considérables mais sans chiffre d'affaires directement localisé dans les pays d'utilisation, les critères classiques comme les revenus et les prix ne sont plus suffisants pour que le droit de la concurrence apprécie le comportement des acteurs. À ce sujet, une doctrine solide sur les services gratuits dans le cadre du droit de la concurrence reste à construire* » [(2)].

De manière générale, il importe que les autorités de régulation de la concurrence, lorsqu'elles ont à statuer sur un cas particulier, prennent mieux en compte la complexité des marchés multiface sur lesquels interviennent les plateformes en particulier les effets de réseau directs et indirects. Aux États-Unis, l'affaire du rachat de *WhatsApp* par *Facebook* a notamment permis à la *Federal Trade Commission*, à l'occasion de l'exercice de ses missions de contrôle des concentrations, de rappeler au réseau social ses obligations en termes de respect de

---

(1) La régulation des plateformes numériques, conférence organisée par la Chaire Innovation & Régulation des Services numériques, Telecom Paris Tech, 7 avril 2015.

(2) Sur ce sujet, voir notamment Estelle Malavolti et Frédéric Marty, « La gratuité peut-elle avoir des effets anticoncurrentiels ? Une perspective d'économie industrielle sur le cas Google », OFCE, *janvier 2013.*

la vie privée de ses utilisateurs. Ce faisant, l'autorité chargée du commerce américain s'écarte d'une approche « en silo » pour apporter une réponse globale aux problèmes soulevés par les grandes plateformes au-delà du seul spectre de la concurrence. Cette démarche, qui semble par ailleurs particulièrement adaptée dans un contexte de porosité forte entre les dimensions personnelles et économiques des données [(1)], mériterait d'être dupliquée, en associant mieux les missions confiées à l'ARCEP, la CNIL et d'autres autorités administratives indépendantes sectorielles dans l'instruction et l'examen des dossiers dont a à connaître l'Autorité de la concurrence afin de prendre en compte les spécificités des secteurs dans la définition des marchés pertinents et les indicateurs de puissance de marché.

Recommandation n° 88

Améliorer l'efficacité du droit de la concurrence face aux problématiques spécifiques de l'économie numérique :

– encourager le recours à des mesures conservatoires destinées à empêcher que des situations n'évoluent de manière irréversible au détriment des partenaires des plateformes ;

– proposer une adaptation des critères d'examen des opérations de concentration et de qualification d'une position dominante afin de mieux appréhender, au-delà du seul chiffre d'affaires, un potentiel de croissance non monétisé assis sur la collecte et le traitement de données à caractère personnel ou l'existence d'une base d'utilisateurs susceptibles de générer de la valeur et des effets de réseau importants ;

– s'écarter d'une approche « en silo » de la régulation concurrentielle pour apporter une réponse globale aux problèmes soulevés par les plateformes, notamment à l'occasion du contrôle des concentrations.

ii. Le droit commercial

Le fait qu'une entreprise soit une plateforme et qu'elle devienne un « *gatekeeper* » incontournable vers certains contenus, services ou applications ne constitue pas en soi un critère suffisant pour faire jouer le droit de la concurrence : pour examiner les comportements unilatéraux des plateformes, encore faut-il qu'elles détiennent une position dominante, dont la caractérisation est soumise à un standard exigeant qui n'est pas satisfait par le fait que l'activité en cause soit une activité de « plateforme ». Sans être nécessairement dominantes, certaines plateformes peuvent pourtant utiliser leur pouvoir de marché pour fausser une concurrence par les mérites. Les règles actuelles du droit européen de la concurrence n'appréhendant pas les pratiques restrictives de concurrence entre

(1) *Conseil national du numérique*, Neutralité des plateformes, Réunir les conditions d'un environnement numérique ouvert et soutenable, op. cit.

professionnels, ni les déséquilibres significatifs qui sont induits par certaines pratiques contractuelles, certaines plateformes numériques peuvent bousculer l'équilibre d'un marché sans pour autant être inquiétées du fait de leurs comportements.

L'approche par le droit commun pourrait donc également passer par **un renforcement de la protection de l'équilibre des contrats entre entreprises commerciales**. Le Conseil national du numérique préconise lui aussi de « *réinvestir le droit commercial pour remédier aux limites des outils de concurrence* » et de « *mettre en place* ***des principes adaptés à l'économie numérique qui s'inspirent du droit des pratiques restrictives de concurrence*** » (1) et en particulier de la notion de déséquilibre significatif, déjà prévue par le code de commerce afin d'appréhender l'absence de réciprocité ou la disproportion dans les obligations entre les parties. De telles dispositions existent en droit français et visent à prévenir les déséquilibres contractuels. Certaines décisions prises à l'égard de plateformes ont été rendues sur le fondement de ces dispositions (2). Appliquées aux plateformes, ces règles ne supposent pas de contraintes de définition de marché, de caractérisation d'une position dominante et de l'effet anticoncurrentiel d'une pratique sur le marché et se concentrent davantage sur la nature des relations entre entreprises. **Harmonisées au niveau communautaire, ces règles pourraient constituer un levier puissant pour prévenir les abus auxquels peut conduire un pouvoir de négociation excessif**.

Comme le souligne le Conseil national du numérique, « *l'élaboration des moyens d'action adaptés à l'économie numérique appellera un processus nécessairement long, fruit d'allers et retours entre différents outils juridiques (loi, contentieux, contrat), à l'image de ce que l'on observe dans le secteur de la grande distribution depuis des décennies* » (3). À cet égard, la Commission met en garde contre le risque d'une course à l'adaptation permanente du droit aux stratégies des acteurs. Comme le Président de l'Autorité de la concurrence l'a souligné lors de son audition, le bilan qui peut être fait de l'application de l'article L. 442-6 du code de commerce dans le rééquilibrage des relations entre fournisseurs et distributeurs dans le secteur du commerce de détail invite à une grande prudence. Les acteurs économiques ont su déjouer l'application de la norme en faisant évoluer leurs pratiques commerciales, et le législateur a été pris dans une course visant à adapter constamment le dispositif pour appréhender ces pratiques commerciales changeantes, sans atteindre les objectifs recherchés (le pouvoir de négociation de la grande distribution n'a jamais été aussi fort) et au détriment du consommateur pour qui les prix ont augmenté. C'est pourquoi il importe en ce domaine de **mettre en place des règles simples, robustes et adaptables**.

---

(1) *Conseil national du numérique,* Ambition numérique, op. cit., *p. 70 ; Rapport sur la neutralité des plateformes,* op. cit., *p. 29.*

(2) *Il en va ainsi, par exemple, du site* Kelkoo *condamné pour pratiques commerciales déloyales le 24 juillet 2014 ou du site* Expedia, *condamné pour avoir imposé des contrats déséquilibrés à l'égard des hôtels qu'il référençait.*

(3) *Conseil national du numérique,* Ambition numérique, op. cit., *p. 72.*

Recommandation n° 89

Agir pour la mise en œuvre d'un dispositif européen interdisant certaines pratiques commerciales restrictives afin de prévenir ou de sanctionner les comportements visant à :

– obtenir d'un partenaire commercial un avantage quelconque ne correspondant à aucun service commercial effectivement rendu ou manifestement disproportionné au regard de la valeur du service rendu ;

– soumettre un partenaire commercial à des obligations créant un déséquilibre significatif dans les droits et obligations des parties ;

– obtenir, sous la menace d'une rupture brutale totale ou partielle des relations commerciales, des conditions manifestement abusives concernant notamment les prix, les délais de paiement, les modalités de vente.

iii. Le droit de la consommation

Le code de la consommation contient de nombreuses dispositions visant la protection des consommateurs. L'une des plus importantes est celle interdisant les « clauses abusives ». Le 7 novembre 2014, la Commission des clauses abusives a adopté une recommandation concernant des clauses abusives figurant dans les conditions d'utilisation de réseaux sociaux [(1)]. L'approche de la Commission intègre dans le concept de « clause abusive » des dispositions contractuelles contrevenant au principe de loyauté ainsi que des celles qui sont contraires à la loi dite « Informatique et libertés ».

En ce qui concerne le renforcement des obligations des plateformes à l'égard des utilisateurs, il peut passer par une adaptation du droit de la consommation.

La loi pour la croissance, l'activité et l'égalité des chances économiques a introduit un nouvel article L. 111-5-1 dans le code de la consommation qui renforce les obligations de loyauté des plateformes numériques à l'égard des consommateurs. Cet article prévoit que toute plateforme numérique, définie comme « *toute personne dont l'activité consiste à mettre en relation, par voie électronique, plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un bien ou d'un service, est tenue de délivrer une* ***information loyale, claire et transparente sur les conditions générales d'utilisation du service d'intermédiation et sur les modalités de référencement, de classement et de déréférencement des offres mises en ligne*** ». Tout manquement est passible d'une amende administrative dont le montant ne

(1) http://www.clauses-abusives.fr/recom/index.htm.

peut excéder 75 000 euros pour une personne physique et 375 000 euros pour une personne morale [(1)].

Afin de renforcer leur effectivité, il serait souhaitable d'inscrire ces principes dans un texte européen. Ils pourraient être complétés par d'autres dispositions visant notamment à garantir l'interopérabilité.

iv. Le droit de la protection des données à caractère personnel

Le droit français de la protection des données à caractère personnel a déjà été appliqué à des plateformes [(2)].

L'objectif d'adaptation du droit commun à la réalité des plateformes est également au cœur du projet de règlement européen sur la protection des données à caractère personnel. Les obligations d'édicter des CGU lisibles en matière d'exploitation des données à caractère personnel, d'assurer l'application effective de l'*opt-in*, d'interdire l'utilisation discriminante des données dans les politiques de prix, l'obligation d'assurer une plus grande portabilité des données que le Conseil national du numérique rattache à la notion de « loyauté des plateformes » relèvent du champ de ce projet de règlement. Ces règles s'appliqueront de plein droit aux plateformes mais ne sauraient se limiter à elles.

De manière générale, le projet de règlement va permettre de renforcer l'effectivité du droit de la protection des données à caractère personnel à l'égard des grandes plateformes en s'appliquant dès lors qu'un résident européen sera concerné et en adaptant le niveau des sanctions applicables à ces acteurs.

v. Le droit fiscal

Les nouveaux modèles économiques du numérique ont permis à certains acteurs économiques internationaux, en particulier les grandes plateformes, de limiter la charge fiscale dans les pays de consommation où ils réalisent une grande part de leur chiffre d'affaires en s'implantant dans des États à fiscalité réduite ou nulle. Cette optimisation fiscale, régulièrement dénoncée en France comme dans d'autres pays, porte un fort préjudice aux finances des États. De surcroît, elle occasionne des **distorsions de concurrence** entre entreprises. Il convient donc d'adapter la fiscalité et d'agir contre l'optimisation fiscale, en privilégiant une action coordonnée aux niveaux international et européen.

---

(1) Article 134 de la loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques.

(2) Se fondant sur le principe de « loyauté », la CNIL a ainsi condamné le site Les Pages Jaunes *pour la collecte de données à caractère personnel à partir de pages publiques de réseaux sociaux (délibération de la formation restreinte n° 2011-203 du 21 septembre 2011 portant avertissement à l'encontre de la société Pages Jaunes). La sanction de la CNIL a été confirmée par le Conseil d'État (CE, 12 mars 2014, n° 353193). La CNIL a également sanctionné* Google *le 3 janvier 2014 pour les modifications que le site a apportées à ses conditions d'utilisation en matière de confidentialité (délibération de la formation restreinte n°2013-420 prononçant une sanction pécuniaire à l'encontre de la société Google Inc.).*

À cet égard la France préconise un assujettissement des opérateurs économiques aux règles générales sous réserve des spécificités du secteur, l'idée étant de taxer les revenus qui ne le seraient pas, le cas échéant, par l'imposition d'une taxe assise sur la « présence digitale » [(1)]. La France préconise une action portant sur l'ensemble des entreprises multinationales, qui s'articule entre, d'une part, un renforcement de la transparence et, d'autre part, le renforcement des règles communes en matière de fiscalité directe en vue de parvenir à une taxation effective des revenus générés par l'activité, y compris numérique, au sein de l'Union européenne.

Recommandation n° 90

Adapter les différentes branches du droit commun afin de mieux appréhender les problématiques propres aux plateformes numériques :

– renforcer l'application des obligations de transparence et de loyauté des plateformes à l'égard des consommateurs ;

– poursuivre l'objectif d'encadrement des pratiques des plateformes en matière d'utilisation des données à caractère personnel dans le cadre du projet de règlement européen relatif à la protection des données à caractère personnel ;

– adapter la fiscalité à l'ère numérique et lutter contre l'optimisation fiscale à laquelle se livrent les grandes plateformes en privilégiant une action coordonnée aux niveaux international et européen.

b. Une approche par la mise en place d'une régulation spécifique

i. De nombreux acteurs et observateurs appellent à la mise en place d'une régulation spécifique de ces acteurs.

Cet appel à la mise en place d'une régulation spécifique se fonde sur **l'idée que le droit commun, et en particulier le droit de la concurrence, ne permet pas de répondre pleinement aux enjeux posés par les grandes plateformes de l'économie numérique** (voir l'encadré ci-après).

En effet, le droit de la concurrence intervient majoritairement *ex post* en réaction à un comportement anti-concurrentiel et offrirait donc, selon certains, des solutions trop tardives au regard de la rapidité avec laquelle les positions de marché évoluent dans le secteur numérique.

Par ailleurs, le droit de la concurrence, même s'il peut y contribuer, ne vise pas à défendre **le pluralisme et le droit à l'information**. Des règles spécifiques concernant les médias audiovisuels et la presse existent à cet égard. **La poursuite de cet objectif pourrait donc selon certains justifier que des**

---

(1) Note des autorités françaises sur les enjeux du marché unique du numérique pour l'Union européenne, 23 mars 2015.

obligations particulières soient imposés à certains acteurs occupant un rôle clé dans l'accès aux informations, en particulier le moteur de recherche *Google*.

De nombreux acteurs préconisent la mise en place d'une régulation spécifique des plateformes

Dans sa communication du 6 mai 2015 (1), la **Commission européenne** relève que « *certaines plateformes en ligne sont désormais devenues des acteurs économiques à part entière dans de nombreux secteurs de l'économie* » et que « *la manière dont elles utilisent leur puissance sur le marché pose un certain nombre de problèmes qui méritent une analyse dépassant la seule application du droit de la concurrence dans des cas spécifiques* ».

Un **rapport d'information de Mme Catherine Morin-Desailly**, fait au nom de la Commission des affaires européennes du Sénat en mars 2013, intitulé *L'union européenne, colonie du monde numérique ?* propose d'appliquer une régulation *ex ante* à de grands acteurs tels que *Google* ou *Facebook*.

Dans son rapport annuel 2014, le **Conseil d'État** rappelle que selon la doctrine définie par la Commission en matière de communications électroniques, une régulation *ex ante* peut être instaurée lorsque la concurrence n'est pas effective en raison de la position dominante d'une ou plusieurs entreprises et lorsque les recours fondés sur le droit général de la concurrence ne parviennent pas à y remédier. Le Conseil d'État indique qu'une régulation *ex ante* « *pourrait être envisagée* » dans la mesure où « *ces deux conditions semblent ici réunies pour certains secteurs, au vu notamment de la lenteur des procédures européennes* » (2).

L'*Open Internet Projet*, syndicat regroupant de grands éditeurs européens, défend la mise en place d'une régulation spécifique des grandes plateformes numériques, en particulier de Google.

Dans une contribution à la consultation du Conseil national du numérique sur la loyauté entre les acteurs économiques, **l'ARCEP** appelle également à la mise en place d'une régulation des « *grands acteurs structurants pour l'économie numérique* » (3).

Une note des **autorités françaises** du 23 mars 2015 relative aux enjeux du marché unique pour l'Union européenne se prononce clairement en faveur de la mise en place d'une régulation spécifique européenne des « *plateformes numériques structurantes pour l'économie* ».

(1) Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la stratégie pour un marché unique numérique en Europe, COM/2015/0192 final, 6 mai 2015.

(2) Conseil d'État, op. cit., *p. 224.*

(3) http://www.arcep.fr/fileadmin/reprise/communiques/communiques/2015/2015-02_CNNum_ARCEP_loyaute_VF.pdf.

ii. Les difficultés posées par la mise en place d'une telle régulation ne doivent pas être sous-estimées, à commencer par la définition de son champ.

Alors que la régulation de la neutralité des réseaux est facilitée par l'existence historique d'une régulation sectorielle des télécoms, secteur clairement identifié, la principale difficulté à laquelle se heurte la mise en place d'une régulation des plateformes est en effet d'identifier le périmètre des acteurs à réguler et les obligations auxquelles ils doivent être soumis, la première définition étant tributaire de la seconde.

MM. Thierry Pénard et Winston Maxwell [1], opposés à la mise en place d'une régulation spécifique, soulignent en particulier que « *les plateformes sont multiformes : elles sont tout à la fois des infrastructures, des places de marchés, des fournisseurs d'applications et de contenus, et des modèles d'affaires. Le terme "plateforme" regroupe une multitude de services différents, relevant de secteurs variés, chacun obéissant à un encadrement juridique spécifique. Une plateforme est par ailleurs un modèle d'affaires utilisé aussi bien dans le monde physique que dans le monde numérique. La "chose" à réguler est mal définie et potentiellement vaste. Deuxièmement, les marchés numériques évoluent très rapidement et il est très probable que les acteurs dominants d'aujourd'hui ne seront pas ceux de demain, encore moins ceux d'après-demain. Personne ne peut prédire comment seront structurés les marchés dans les prochaines années, quels en seront les points d'entrée et comment évolueront les préférences des utilisateurs. Prenons comme exemple la « plate-forme » d'*iTunes. *Dans les années 2000, les pouvoirs publics étaient très inquiets de la position d'Apple et de sa capacité à organiser le marché de la musique. En quelques années, les cartes ont été redistribuées par le simple jeu de l'innovation, avec l'essor des services de streaming (*Deezer *et* Spotify*). Les effets « winner-takes-all » qui peuvent assurer le succès d'une plateforme en très peu de temps, peuvent aussi en accélérer le déclin au profit de nouveaux acteurs* ».

En ce qui concerne le périmètre des « plateformes » à réguler, diverses options sont avancées. Certains invitent à cibler les plateformes en position dominante, notion qui a le mérite d'être clairement définie. D'autres invitent à la dépasser.

C'est le cas de l'ARCEP, dans sa contribution précitée, qui a recours à la notion de « *grands acteurs structurants pour l'économie numérique* », notion qui reste à définir. Selon l'Autorité, la définition du champ des acteurs à réguler « *compte tenu de leur caractère structurant dépassant les seuls enjeux concurrentiels ne pourra sans doute pas procéder uniquement des principes du droit de la concurrence et, notamment de la notion de position dominante* ».

Le Conseil national du numérique propose pour sa part de définir une catégorie de **plateformes « *dotées de la plus forte capacité de nuisance* » qui se verrait imposer certaines obligations spécifiques**. Ces dernières seraient définies par « *le recours à un faisceau d'indices* ». La Commission n'est pas favorable à cette notion de « *plus forte capacité de nuisance* » qui, comme l'a souligné M. Bruno Lasserre, président de l'Autorité de la concurrence lors de son audition, est une notion essentiellement morale et non juridique.

Les autorités françaises, dans la note précitée, proposent également de cibler « *les plateformes numériques structurantes pour l'économie* », lesquelles seraient définies sur la base de critères cumulatifs. Trois critères sont avancés. Il doit s'agir de :

---

(1) « Réguler les plateformes : une fausse bonne idée », L'Opinion, *23 avril 2015.*

– services de la société de l'information, destinés à des personnes ou des entreprises résidant dans un ou des États membres de l'Union européenne ;

– fournis pas des entreprises exerçant à titre professionnel une **activité économique d'intermédiaire sur un marché biface** dans le domaine de la société de l'information ;

– et dont le positionnement sur le marché permet à ces entreprises d'adopter des comportements indépendants (par exemple la définition de conditions économiques et commerciales) vis-à-vis de leurs concurrents, de leurs clients et des consommateurs en général.

Dans ce périmètre, « *seraient ainsi visés certains moteurs de recherche ; places de marchés, y compris de vente ou diffusion de contenus culturels ; magasins d'applications et* ***systèmes d'exploitation des équipements terminaux voire terminaux eux-mêmes*** *; à venir des objets connectés* ».

Il est intéressant de relever que la définition proposée des « plateformes » est recentrée sur la notion économique de marché biface et **étendue aux systèmes d'exploitation des équipements terminaux, voire aux terminaux eux-mêmes, ce dont on peut se féliciter**.

Pour les autorités françaises, « *le caractère structurant d'une plateforme pourrait être caractérisé au niveau européen en se fondant sur des critères les plus objectifs possibles (par exemple, d'audience ou de fréquentation) afin de limiter les possibilités d'interprétation et les difficultés en résultant* ».

Mme Marie-Anne Frison-Roche, spécialiste du droit de la régulation, propose quant à elle une approche originale consistant à dépasser la notion de plateforme pour viser une régulation des « entreprises cruciales » [(1)] (voir l'encadré ci-après) à laquelle correspondraient des entreprises comme *Google*, *Facebook* ou *Amazon*.

Une proposition d'approche par la notion d'« entreprise cruciale »

Mme Marie-Anne Frison-Roche identifie une difficulté plus globale du droit à réguler les marchés bifaces : « parce que les marchés biface ne sont pas propres à un secteur, tant que l'on pensera le droit de la régulation en l'enfermant dans un secteur particulier, l'on ne pourra pas penser la régulation des marchés bifaces. En effet, si l'on pense en termes de régulation sectorielle, la régulation est imprégnée d'un objet très concret qui se développe sur tel ou tel secteur (le téléphone, l'électricité, le gaz, le jeu, etc.) » alors que la notion de marché biface est abstraite et transversale.

Selon Mme Marie-Anne Frison-Roche, il serait dangereux de définir une catégorie juridique de « plateformes ». « La difficulté d'une telle définition est qu'elle ne correspond pas à ce que doit être la définition, à savoir une abstraction, mais renvoie à une liste, ce qui n'est pas une définition et posera inévitablement le problème constitué par une situation proche d'un des cas visés mais non identique à celui-ci. Il y aura alors ce que redoutent le

(1) *Marie-Anne Frison-Roche, « Enjeux de régulation d'entreprises cruciales » in* Économie de plate-formes : réguler un modèle dominant ?.

plus les opérateurs, à savoir de l'insécurité juridique. En outre, ce régime spécifique, à savoir une obligation de loyauté, ne serait donc attaché qu'aux entreprises dominantes sur les marchés biface d'internet et pas sur les autres entreprises de même type sur les autres marchés biface, par exemple les entreprises qui proposent des moyens de paiement, lesquelles ne se définissent pas comme des entreprises de « services de référencement et de classement. N'est-ce pas dommage ? Faut-il à ce point créer un droit de l'internet ? Le droit ne perd-il pas sa force à être si peu commun ».

Mme Marie-Anne Frison-Roche propose d'aborder la régulation des plateformes à travers celle, plus générale, des « entreprises cruciales ». « Dans un sens négatif, une entreprise est cruciale si sa disparition cause un choc sur le système économique et social, sa disparition mettant en péril celui-ci. Dans un sens positif, une entreprise est cruciale si le bon fonctionnement du système économique et social dépend de la présence, du bon gouvernement et du bon comportement de cette entreprise. Cette conception négative de l'entreprise cruciale, basée sur l'idée de risque systémique, a fondé l'Union bancaire européenne. La définition positive de l'entreprise cruciale fait quant à elle ressortir que dans une situation de dominance, née d'un marché biface, lorsqu'il s'agit d'accéder à la vie sociale (…) ou d'accéder à l'information, l'entreprise doit être forcée à prendre en compte le groupe social et autrui ». Selon Mme Marie-Anne Frison-Roche, la puissance publique serait légitime, sans que l'État ait à devenir actionnaire, à se mêler de la gouvernance de ces entreprises cruciales et à surveiller les contrats, voire à certifier ceux-ci, comme en finance.

Faire de ces plateformes « structurantes pour l'économie » des cibles pour une régulation spécifique ne participe pas d'une démarche qui viserait à « punir » un quelconque succès, comme il ne s'agit pas de soupçonner systématiquement les plateformes de s'adonner à des pratiques abusives ou contraires à l'intérêt général économique. Une forme de régulation *ad hoc* tendrait plutôt à consacrer leur importance, leur caractère quasi-incontournable, voire universaliste, qui les rend dépositaires d'une partie du bien commun que constitue l'environnement numérique. Dans ces conditions, la Commission ne trouve pas anormal que puissent s'imposer à ces acteurs d'un genre nouveau des obligations particulières, que ce soit en termes de transparence ou de non-discrimination, ce qui implique par exemple d'exiger d'eux qu'ils documentent publiquement et de manière plus complète les algorithmes qu'ils utilisent ou de les soumettre à des obligations en matière de diversité culturelle, notamment le respect de la langue française. Elle note d'ailleurs que c'est une voie qu'a régulièrement empruntée le législateur, notamment dans le domaine des télécommunications où les obligations de publicité et de non-discrimination dans les services d'interconnexion sont différenciées selon la puissance de marché de l'opérateur auxquelles elles s'appliquent (notion d'influence significative sur le marché [(1)]).

La Commission relève toutefois que cette régulation asymétrique des opérateurs puissants de communications électroniques est limitée à certains marchés répondant à un test de trois critères [(2)] et qu'elle doit disparaître à terme

---

(1) Avant-dernier alinéa de l'article L. 37-1 du code des postes et des communications électroniques.

(2) Les trois critères sont l'existence de barrières durables à l'entrée, l'absence d'évolution prévisible du marché et l'insuffisance du droit de la concurrence à traiter les défaillances du marché. Le nombre de marchés a progressivement diminué, passant de 18 à 5 (voir la recommandation de la Commission du 9 octobre 2014 concernant les marchés pertinents de produits et de services dans le secteur des

pour laisser place au droit de la concurrence [1]. L'approche de la régulation appliquée aux opérateurs de communications électroniques semble donc difficilement transposable aux plateformes numériques.

S'agissant des objectifs de la régulation et des droits et obligations qui seraient applicables à ces plateformes, là encore, les approches peuvent être très diverses.

Comme l'a souligné M. Bruno Lasserre, président de l'Autorité de la concurrence, « *c'est, en effet, par là qu'il faut commencer : on ne fait rien de bon quand on n'a pas une idée claire de ce que l'on veut faire. À cet égard,* ***plusieurs finalités sont envisageables, qui ne sont pas exclusives les unes des autres*** *: défense du pluralisme et de la liberté d'expression ; protection des données personnelles et, plus largement, de la vie privée, qui peuvent être mises en danger par certaines pratiques ; protection de l'autonomie et de la liberté de choix du consommateur ; préservation d'un terrain de jeu ouvert et concurrentiel ; promotion d'offres concurrentes, de préférences européennes, face à la domination de géants parmi lesquels on ne trouve que peu d'acteurs européens ; correction d'une inégalité de rapports de force, atténuation d'une situation de dépendance dans laquelle se trouvent les opérateurs économiques vis-à-vis des plateformes dominantes, afin d'aller vers un partage équitable de la valeur* » [2].

Pour l'ARCEP, dans la contribution précitée, « *la nature des obligations pesant sur ces acteurs spécifiques devra tenir compte de l'extraordinaire dynamique du marché et devrait sans doute procéder de* ***principes suffisamment généraux*** *tels que l'équité, l'objectivité, la proportionnalité, voire la non-discrimination* ».

Lors de son audition, M. Jean-Ludovic Silicani, ancien président de l'ARCEP, a évoqué l'hypothèse, parfois envisagée comme alternative à la mise en place d'une régulation spécifique, d'une **extension du champ de la régulation des télécoms à d'autres acteurs, en particulier les fabricants de terminaux et les moteurs de recherche** : « *le principe de neutralité des réseaux s'applique à la relation entre opérateurs de réseaux et utilisateurs de bout en bout, depuis l'interconnexion entre les réseaux et les contenus jusqu'à l'utilisateur final. À cet égard, une question se pose : où ces deux bouts se situent-ils exactement ? L'accès au réseau par les moteurs de recherche entre-t-il dans le champ d'application du principe de neutralité ? À ce stade, ce point n'est pas tranché. À l'autre bout, le terminal final – par exemple le smartphone – entre-t-il dans ce champ*

---

communications électroniques susceptibles d'être soumis à une réglementation ex ante *conformément à la directive 2002/21/CE du Parlement européen et du Conseil relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques 2014/710/UE).*

(1) Considérant 5 de la directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.

(2) Audition du7 juillet 2015.

d'application ? » Cette solution présente l'avantage de la simplicité, certaines obligations au cœur de la notion de neutralité, comme la transparence, l'équité et la non-discrimination, pouvant être transposables aux plateformes.

Les autorités françaises proposent quant à elles de bâtir une régulation en recourant à une liste de « thématiques » plus détaillée, dont on relèvera qu'elles sont centrées sur les notions d'équité, de transparence et de non-discrimination et ne recourent pas à la notion plus floue de « loyauté » :

– transparence et non-discrimination des conditions d'accès aux plateformes ;

– traitement équitable dans les conditions de référencement et transparence des critères de fonctionnement des algorithmes ;

– traitement lisible des résultats sponsorisés et naturels ;

– encadrement des clauses de contraintes tarifaires ;

– prévisibilité des modifications d'API (stabilité des règles et délai préalable d'information en cas de changement) ;

– encadrement de l'accès aux (méta)données utilisées pour le référencement ;

– encadrement des conditions commerciales ;

– transparence sur la localisation géographique des données ;

– encadrement de l'extraction des données (métriques, contenu) et de la portabilité vers une autre plateforme ;

– transparence sur les écosystèmes avec lesquels la plateforme peut interopérer ;

– transparence sur les conditions de licence sur les contenus / données ;

– le cas échéant, respect des obligations liées à la promotion de la diversité culturelle.

Sur l'opportunité de mettre en place une régulation spécifique des plateformes, la Commission n'est pas unanime.

Pour certains membres, il convient de privilégier l'approche par le droit commun. M. Winston Maxwell estime en particulier qu'« *une nouvelle régulation spécifique doit rester une solution de dernier ressort* » (1) et s'appuyer sur une analyse précise des dysfonctionnements du marché et des gains attendus de la régulation ainsi que de ses effets secondaires sur l'écosystème d'internet.

Pour la majorité des membres, l'approche par l'adaptation du droit commun peut être complétée par la recherche d'une régulation spécifique, portant sur les acteurs dominants de l'économie numérique, à commencer par *Google*. La

---

(1) Winston Maxwell et Thierry Pénard, op. cit.

Commission insiste également pour que le champ de la régulation permette d'appréhender la problématique des terminaux.

Cette régulation devra assurer une grande réactivité compte tenu des évolutions très rapides des marchés. Des **principes directeurs suffisamment généraux** pourraient être adoptés au niveau européen et précisés au niveau national, notamment dans le cadre d'un examen, au cas par cas, par le biais de règlements rapides des litiges entre acteurs à l'instar de ceux prévus dans le secteur des communications électroniques, où ce type de procédure s'est avéré très efficace pour construire rapidement et de manière pragmatique des règles du jeu équitables.

En attendant une régulation globale des plateformes au niveau européen, **rien n'interdit au législateur national d'avancer vers des formes de régulation des plateformes au plan national**. À cet égard, on peut noter que le projet de loi relatif à la liberté de création, à l'architecture et au patrimoine comporte des dispositions tendant à mieux réguler les relations et le partage de la valeur entre producteurs phonographiques et plateformes de musique en ligne.

Recommandation n° 91

Pour certains membres de la Commission, il convient de privilégier l'approche par le droit commun et une nouvelle régulation spécifique doit rester une solution de dernier ressort et s'appuyer sur une analyse précise des dysfonctionnements du marché et des gains attendus de la régulation ainsi que de ses effets secondaires sur l'écosystème d'internet.

Pour la majorité des membres de la Commission, l'approche par l'adaptation du droit commun peut être complétée par la mise en place d'une régulation spécifique, portant sur les acteurs dominants de l'économie numérique.

V. DESSINER UNE NOUVELLE FRONTIÈRE ENTRE PROPRIÉTÉ ET COMMUNS

La révolution numérique n'a pas été seulement propice à l'approfondissement et à l'élargissement des droits et libertés de nature politique ou économique. En raison de la décentralisation des ressources de production et des capacités rapides d'échange, elle a sensiblement modifié les modalités de production et d'accès aux contenus réalisés à l'aide du numérique ou rendus accessibles par internet. Cette évolution a été permise, en outre, par l'émergence d'une culture du partage, de la collaboration et de la coopération qui s'est illustrée, dès l'origine, par la conception même d'internet, réticulaire, décentralisée et fondée sur des protocoles d'échanges ouverts. Elle donne lieu à la réalisation en commun d'objets, de protocoles, de logiciels, vecteurs d'une innovation rapide liée à une contribution constante de la communauté à l'amélioration et à l'adaptation de ces objets à leur environnement et ainsi qu'à leur meilleure acceptabilité par les utilisateurs.

Ces mouvements sociaux et techniques profonds vont de pair avec de multiples expressions politiques prônant une meilleure prise en compte de la culture du partage et du caractère essentiel de la préservation des ressources numériques communes contre les **risques d'« enclosure »**, à savoir la diminution - graduelle ou soudaine - de l'accessibilité de ces ressources. Cette revendication se traduit en particulier par un appel de certains acteurs de la société civile à une meilleure reconnaissance et défense de ce qu'il est convenu d'appeler les « communs », appel dont la Commission considère nécessaire de se faire l'écho. Une telle vision a notamment été défendue par M. Daniel Kaplan lors de la présentation devant la Commission du rapport *Ambition numérique* du Conseil national du numérique le 17 juin 2015 : pour que le numérique contribue « *à l'émergence d'une société plus juste, plus égalitaire et plus durable* », il faut, dit-il, « *refaire société par les communs dont internet fait partie* ». Selon ce rapport, « *un commun ou bien commun est une ressource dont les droits d'usage sont partagés : une ressource gérée par une communauté qui fixe des règles de gouvernance afin de protéger et faire fructifier cette ressource* » (1).

Plusieurs types de communs numériques peuvent être distingués :

– **les biens communs structurels ou vecteurs de communication** : il peut s'agir par exemple des logiciels libres ou des infrastructures d'internet – sa structure et son architecture, à l'instar des noms de domaine ou des logiciels de transport des données selon les normes *TCP/IP* qui lui permettent d'exister, font d'internet un bien commun inappropriable, même si l'ensemble des « couches » qui en constituent l'essence ne présentent pas toutes le même « potentiel de commun » (2) (voir le schéma ci-après) ;

---

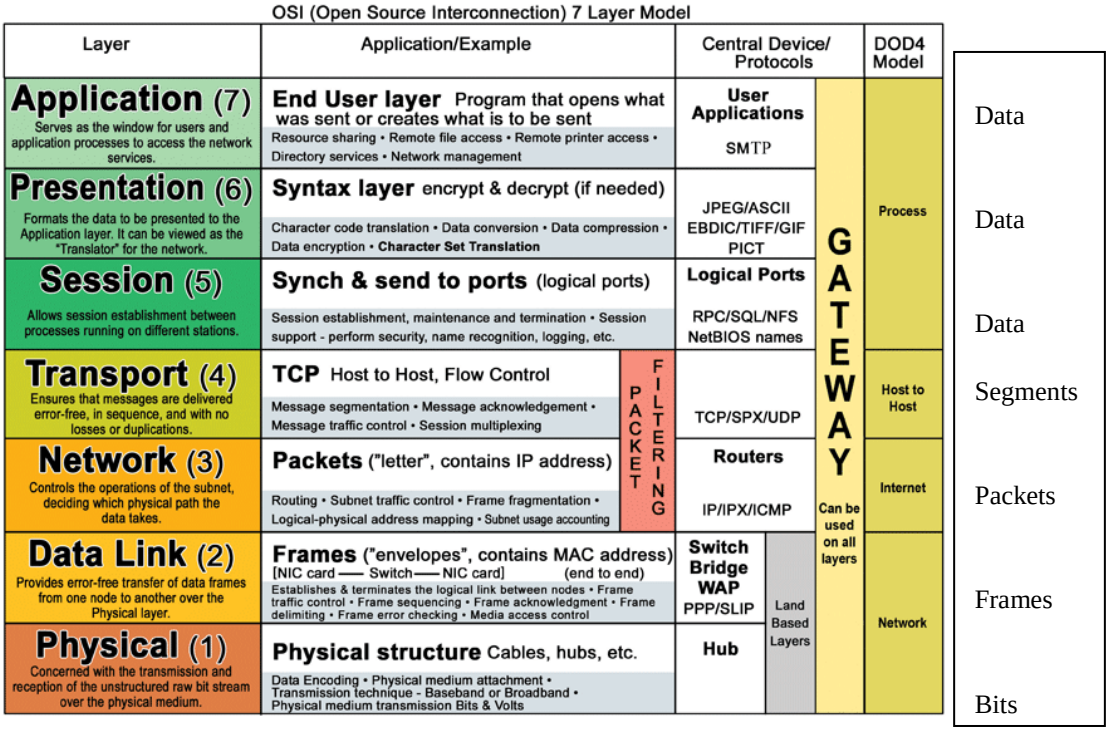
(1) Conseil national du numérique, Ambition numérique, op. cit., *p. 34.*

(2) J. Hofmokl, « Towards an eclectic theory of the internet commons », International Journal of the Commons, *4(1), 226-250, 2009.*

– les **biens communs informationnels** qui visent, non pas les vecteurs de communication, mais les **contenus et connaissances partagées**, au sein desquels on peut trouver de nouvelles formes de médias et de contenus propres ou adaptés à la culture numérique (blog, conversations numériques, wikis, œuvres protégées dont les auteurs ont choisi des modèles volontaires de partage, notamment à travers les licences libres, éléments du domaine public informationnel, données relevant de l'*open data* …).

La Commission partage les conclusions du rapport *Ambition numérique* du Conseil national du numérique selon lesquelles **internet en tant que « *ressource essentielle au développement de nos sociétés tant du point de vue économique que culturel ou social (…) doit être considéré comme un bien commun, ou commun***, *qui ne peut être préempté par les intérêts de certains acteurs, publics ou privés, mais doit bénéficier à la communauté mondiale des utilisateurs* » [(1)]. Le rapport du Conseil national du numérique estime néanmoins qu'internet n'inclut pas les infrastructures physiques des réseaux ou des serveurs, qui sont soumises à des régimes de propriété privée ou, plus rarement aujourd'hui, publique, ce qui montre la difficulté d'aménager un régime commun à l'ensemble garantissant un accès universel au réseau.

Le modèle OSI des couches de l'internet comme biens communs [(2)]



(1) *Conseil national du numérique*, op. cit., *p. 34.*

(2) *Ce tableau est disponible ici ; il figure dans ce rapport dans une version réélaborée par Mmes Francesca Musiani et Mélanie Dulong de Rosnay.*

Partageant le constat selon lequel les communs numériques constituent « *un moteur d'innovation économique et sociale* » dont les bénéfices, aujourd'hui encore trop peu exploités par la société, font l'objet d'un risque de prédation [(1)], la Commission, après avoir clarifié les éléments de terminologie nécessaires à une bonne appréhension du phénomène (**A**), souhaite formuler plusieurs recommandations propres à accompagner cette évolution dans la société numérique (**B**).

A. LE DÉVELOPPEMENT DES COMMUNS NUMÉRIQUES

La notion de communs ne date pas du numérique. Elle a d'abord été identifiée par la littérature économique et juridique à propos des choses naturelles, telles que l'eau, l'air ou certains pâturages, puis progressivement étendue à des objets informationnels, domaine dans lequel elle a pris un essor particulier en raison du caractère potentiellement inépuisable de ces ressources.

Le débat contemporain autour des communs [(2)] peut être daté de la critique suscitée par un article publié en 1968 par Garrett Hardin développant une théorie de la « tragédie des biens communs » [(3)] qui justifierait l'allocation de la propriété privée. Selon lui, dans un *commons*, tous les membres de la communauté ont le privilège d'utilisation de la ressource, sans disposer cependant du droit d'exclure un quelconque membre de la jouissance. L'auteur y mettait en évidence la surexploitation qu'engendre l'utilisation illimitée d'une ressource commune, dans la mesure où chaque utilisateur adoptera en principe le comportement qui lui assure le plus de profit, sans souci du partage avec autrui, et en concluait que seule la propriété privée pouvait garantir le maintien de la ressource.

En réaction à cette analyse qui ne distinguait pas selon que la ressource est mise en libre accès ou fait l'objet d'une propriété commune, plusieurs auteurs dont Elinor Ostrom, prix Nobel d'économie, ont fait valoir que **les communs n'étaient pas équivalents à une absence de droits** (« *Common property is not no one property* ») mais qu'un commun faisait l'objet d'une régulation articulant les droits d'usage sur la ressource et que, contrairement aux conclusions de Garrett Hardin, il n'était pas démontré que la propriété privée garantisse mieux la préservation optimale de la ressource et l'intérêt commun qu'une autre forme de **gouvernance des communs** (voir l'encadré ci-après).

---

(1) Conseil national du numérique, op. cit., *p. 277.*

(2) Pour une analyse historique de cette construction scientifique de la théorie des communs à l'ère contemporaine, voir B. Coriat, « Le retour des Communs. Sources et Origines d'un Programme de Recherche » ; pour une analyse soutenue de l'analyse des communs, voir M.T. Sanou, Le domaine public en droit d'auteur ; ébauche d'un régime pluridimensionnel pour les pays membres de l'OAPI, *thèse Namur, 2015, sous la direction de S. Dusollier.*

(3) G. Hardin, « The Tragedy of the Commons », Science, *13 December 1968, vol. 162, n° 3859, pp. 1243 – 1248 disponible ici.*

La théorie des communs

Pour **Elinor Ostrom** [1], le *Common Pool Resource* (CPR), à savoir la ressource mise en commun, désigne une **ressource naturelle ou artificielle** constituée d'un stock [2] (*resource system*) et d'un contenu composés d'éléments (*resource unit*). Il est **situé à mi-chemin entre le bien privé et le bien public** [3] ; il revêt la caractéristique d'un bien public, au sens économique, en raison de la difficulté d'ériger des moyens physiques ou institutionnels pour exclure des individus du bénéfice de la ressource, compte tenu de la nature du bien [4] qui est suffisamment large pour que de multiples acteurs puissent l'utiliser simultanément [5]. L'assimilation au bien privé apparaît quand la ressource génère une quantité finie d'unités, de sorte que la consommation ou la capture d'une unité réduit la quantité disponible pour les autres. Dans ce cas, ses composantes sont « rivales » et le commun peut faire l'objet de congestion, de pollution, de surexploitation et de destruction, à moins que des limites ne soient fixées et renforcées par une gouvernance collective du commun.

Initialement construite autour de ressources naturelles épuisables, **la théorie des communs s'est ensuite progressivement élargie à des choses intangibles ou de nature intellectuelle**. Charlotte Hess [6] a dressé une cartographie des différents emplois de la notion de *commons*, en distinguant notamment les *new commons* par opposition aux *traditional commons*, *new commons* parmi lesquels on compte **les biens communs de la connaissance** (*knowledge commons*), **les biens communs culturels** (*cultural commons*) **et les biens communs globaux** (*global commons*). Elle a également montré la diversité des régimes susceptibles de s'appliquer aux communs selon les caractéristiques des ressources et leur organisation : gratuits ou non ; rivaux ou non rivaux ; susceptibles d'extinction ou reconstituables ; remplaçables ou non. Ils peuvent être globaux, locaux ou quelque part entre les deux. Les communs ne sont pas antinomiques avec la propriété et peuvent même être le sujet d'une combinaison de droits de propriété.

(1) E. Ostrom, Governing the Commons : The Evolution of institutions for Collective Action, op. cit., *pp. 30 et s.*

*(2) Cette réserve (*stock *ou* facility*) est ce qui génère les composantes de la ressource (*resource unit*) et les bénéfices. Les exemples de* resource system *sont les rivières, les systèmes d'irrigation, les forêts. Un CPR peut aussi être une ressource produite pour une utilisation commune tel internet. E. Ostrom,* op. cit., *pp. 30 et s. ; E. Ostrom et C. Hess, « Artifacts, Facilities and Content : Information as a Common Pool Resource »,* Law and contemporary problems, *p. 121.*

(3) Un autre concept, celui des semi commons, *vise les ressources dans lesquelles interagissent des régimes de propriété privée et les communs. Ces différents régimes de propriété correspondent aux différents usages qui sont faits de la ressource dont certains attributs se prêtent à la propriété privée et d'autres aux communs. E. Bertacchini, « Biotechnologies, seeds and semicommons », p. 7 et pp. 11 et s, disponible sur http://ssrn.com/abstract=960747.*

(4) R. Wade, « The management of common property resources : collective action as an alternative to privatization or state regulation », 11, Cambridge Journal of Economics, *1987, pp. 96 et s. ; D. Feeny and al., « The tragedy of the Commons : Twenty-Two Years Later »,* Human Ecology, *vol. 18, n°1, 1990, p. 3.*

(5) E. Ostrom, « Reformulating the Commons », Swiss Political Science Review *6(1), pp. 29-30. Voy. R. Wade,* op. cit., *pp. 96 et s.; B. E. Burke, « Hardin Revisited : A Critical Look at Perception and the Logic of the Commons », 29,* Human Ecology, *n°4, 2001, p. 453 : «* The biophysical characteristics of a resource can create a commons despite societal attempts to privatize that resource, such as with large bodies of waters, rivers, fish, and other wildlife and air. Their fluidity makes it difficult to divide these into parcels with distinct bundles of property rights ».

(6) C. Hess, « Mapping New Commons », presented at The Twelfth Biennial Conference of the International Association for the Study of the Commons, *Cheltenham, UK, 14-18 July, 2008, p.13. L'auteure a tenté d'en donner un résumé en ces termes : «* (…) some commons are free and sometimes not. They are a birthright and the common heritage of humankind (the atmosphere and the oceans) but they are also local playgrounds or a condominium. They may be rival (roads, health care) or they may be non rivalrous (public art, knowledge). They may be exhaustive (oil, biodiversity) or replenishable (gardens). They may be replaceable (hospital) or irreplaceable (landscapes). They may be global, local, or somewhere in between. And, commons like common-pool resources (economic goods), may have any combination of property rights » *(cf. p. 37).*

Au-delà de la diversité des déterminants de la chose et des mécanismes d'allocation, s'affirme néanmoins un élément caractéristique des communs, à

savoir **l'organisation du partage de la ressource**, que ce soit au sein d'une nation, d'un groupe ou d'une communauté qui ont les mêmes valeurs et intérêts.

À l'ère numérique **la notion de communs s'est étendue** (1) : il ne s'agit plus d'un ensemble de choses préexistantes et inappropriables par nature mais de productions de biens intangibles **mis éventuellement de manière volontaire au service de tous**. Les risques de « tragédie des communs », c'est-à-dire d'épuisement de la ressource par surexploitation, sont d'autant moins présents pour ces biens qu'ils sont souvent non rivaux, c'est-à-dire que l'usage par une personne n'affecte pas l'usage par une autre.

Les communs numériques se développent en synergie avec une sphère d'activités non marchandes, notamment parce que leur usage libère un accès non marchand à la culture et aux connaissances. Tendanciellement, les acteurs des communs affichent une préférence pour la valeur d'usage et la reconnaissance de la contribution par rapport à la valeur d'échange. Le choix de recourir aux communs peut également conduire à une amélioration des processus incrémentaux de production par la mise en commun rapide et mondiale des ressources et connaissances. Les biens communs sont devenus, selon M. Yochai Benkler, la base d'un mode de production par les pairs qui a des « *avantages systématiques sur les marchés et les hiérarchies managériales quand l'objet de production est l'information ou la culture* » (2).

L'importance des communs à l'ère numérique résulte de **plusieurs changements** :

– **des activités qui étaient réservées à de grandes organisations ou à des industriels sont aujourd'hui à la portée d'individus ou de groupes les réunissant avec un investissement relevant pour chacun de la consommation ordinaire** : il en est ainsi dans le champ de la production logicielle, de la création et de la publication de contenus dans les médias, de la production collaborative d'encyclopédies et plus généralement de répertoires des connaissances, de certaines activités scientifiques et de l'innovation, y compris dans certains champs de la production matérielle avec le développement des imprimantes 3D ;

– **la rareté se déplace vers l'attention disponible**, rare au niveau de chaque individu en raison de contraintes de temps.

La croissance exponentielle de ces productions déstabilise les modèles commerciaux fondés sur la rareté de l'offre et la restriction de l'accès. **Ces mutations exigent une adaptation profonde de nos représentations afin d'organiser une cohabitation et d'encourager les synergies entre l'économie marchande et les pratiques non marchandes**, entre les droits exclusifs et

---

(1) M. Clément-Fontaine, « Le renouveau des biens communs : des biens matériels aux biens immatériels », in Les modèles propriétaire au XXIème siècle, *Actes du colloque international organisé par le CECOJI, LGDJ 2012, pp. 52 et s.*

(2) Y. Benkler, « Coase's Penguin or Linux and the Nature of the Firm », Yale Law Journal *(112), 2002.*

l'affirmation des communs. La Commission estime qu'il convient de trouver de nouvelles articulations entre ces modèles et de mieux prendre en compte les communs dans les indicateurs de richesse.

Enfin, les catégories juridiques s'avèrent parfois inadaptées pour appréhender le phénomène. De nombreux auteurs et chercheurs (1) ont proposé diverses pistes afin de donner un statut positif en droit aux communs. Des initiatives multiples se sont déjà développées au plan international pour donner corps à cette notion (2), notamment à propos des productions de l'esprit dont les auteurs ont choisi de privilégier la mise en partage de leurs productions plutôt que d'avoir recours à des mécanismes d'exclusion.

B. RENFORCER LA PLACE DES COMMUNS DANS LA SOCIÉTÉ NUMÉRIQUE

Afin de renforcer la place des communs dans la société numérique et ainsi faire de la révolution numérique un facteur d'émancipation des individus, la Commission s'est intéressée à plusieurs questions : le statut juridique qu'il convenait de leur donner (**1**), la conciliation des droits ou capacités d'usage et des droits de propriété intellectuelle (**2**), les droits des créateurs au titre de l'exploitation numérique de leurs œuvres (**3**) ainsi que les conditions d'exploitation et de partage des connaissances scientifiques (**4**).

1. Donner un statut de droit positif aux communs et au domaine public

La Commission souligne que la reconnaissance des communs est encore balbutiante en droit français, tant celui-ci est attaché à la représentation du rapport d'une chose à un individu à travers la figure de la propriété, envisagée comme un droit d'exclure autrui de sa chose (3). Même lorsque la loi évoque le domaine public, il est en fait question d'un droit de propriété exclusif au profit d'une collectivité publique dotée de la personne morale (État, collectivités territoriales). Quant au domaine public informationnel lié à l'absence de droits de propriété

---

(1) *Voir notamment : Séverine Dusollier, « Scoping study on copyright and related rights and the public domain », 2010 et le séminaire du Vecam « Un statut juridique pour les communs » organisé le 19 mai 2015 ; Philippe Aigrain, « Towards a positive recognition of commons-based research and innovation in international norms », in* New Tools for the Dissemination and Knowledge and the Promotion of Innovation and Creativity : Global Developments and Regional Challenges, *séminaire international, Bibliothèque d'Alexandrie, Égypte, 7-8 septembre 2006 ; Lionel Maurel, « I Have a dream : une loi pour le domaine public en France »,* S. I. Lex, *27 octobre 2012 ; Judith Rochfeld, « Quel(s) modèle(s) juridiques pour les « communs » ? Entre élargissement du cercle des propriétaires », in* Propriété et communs, Les nouveaux enjeux de l'accès et de l'innovation partagés, *seminaire international, Paris, Propice, avril 2013.*

(2) *Voir notamment les travaux de Communia.*

(3) *Sur l'ensemble de la question, voir M. Clément-Fontaine,* L'œuvre libre, *Larcier, 2015 ; J. Rochfeld, « Penser autrement la propriété : la propriété s'oppose-t-elle aux « communs » ? »,* Revue Internationale de droit économique, *2014/3 Tome. XXVIII, p. 140. Par contraste avec nos représentations de la propriété, le commun appelle une conception de la propriété inclusive, c'est-à-dire apte à organiser l'accès de la communauté au bien d'une communauté. Sur ce point, voir S. Dusollier, « The commons as a reverse intellectual property-from exclusivity to inclusivity », in H. R. Howe, J. Griffiths,* Concepts of Property in Intellectual Property, *Cambridge, University Press, 2013, p.258-281.*

intellectuelle, il ne fait l'objet d'aucun statut juridique propre et se cantonne, pour l'heure, à être reconnu comme une catégorie par défaut, recueillant des objets divers qui ne sont pas tous également protégés contre un processus de privatisation. Enfin, les licences libres par lesquelles les auteurs proposent des modalités de partage de la ressource ne font l'objet d'aucune prise en compte particulière, bien que certaines n'apparaissent pas toujours en pleine conformité avec les dispositions d'ordre public du droit français [(1)].

La Commission estime, en premier lieu, que **la reconnaissance des communs numériques procède avant tout d'une option politique**, déterminée notamment par le choix de soumettre l'objet à un mécanisme de propriété privative, d'en rejeter au contraire l'appropriation ou de déterminer un modèle mixte de cohabitation entre usages exclusifs et usages partagés ou inclusifs. Elle souligne que ces choix peuvent partiellement échapper à la compétence du législateur français en raison du caractère international de la ressource ou de la volonté spontanée des acteurs de se conformer à un modèle de non-réservation volontaire et nécessitent, à cet égard, des réponses variées.

Dans ce contexte, la Commission considère pertinent de **promouvoir une reconnaissance positive des communs qui garantisse que la ressource numérique puisse être partagée conformément à son utilité et à sa destination communes d'une part, et qui organise les prétentions respectives des acteurs de manière à éviter que la reconnaissance éventuelle d'un droit exclusif ne prive la collectivité de l'accès aux communs, d'autre part**.

Recommandation n° 92

Le développement des communs numériques appelle leur reconnaissance positive dans le droit français, de manière à garantir l'accès à la ressource commune et son partage équitable, contre les éventuelles revendications d'exclusivité.

La Commission considère, en second lieu, que la reconnaissance d'un statut juridique aux communs numériques, dont on a souligné la diversité, suppose de s'accorder sur ses finalités essentielles. En première approche, elles consistent à **organiser l'accès et l'usage de la ressource**, en assurer la **conservation, la pérennité** et la **transmission** et, si possible, à permettre une **participation large à l'évolution de la ressource par processus incrémental** (au développement d'un logiciel ou à l'amélioration d'une invention) [(2)]. La Commission rappelle que plusieurs mécanismes existants en droit français semblent aptes à appréhender ces objectifs, mécanismes qui vont de la propriété privée exclusive à la non-

---

(1) Sur cette question, voir notamment les travaux du Conseil supérieur de la propriété littéraire et artistique, La mise à disposition ouverte des œuvres de l'esprit, *rapport de V-L. Benabou, J. Farchi, D. Botteghi, 2007, disponible sur le site du ministère de la Culture. Voir également sur les licences libres B. Jean,* Option libre, Du bon usage des licences libres, *Framabook, 2011.*

(2) B. Coriat, « Des communs "fonciers" aux communs informationnels. Traits communs et différences », Séminaire Propice, 2013, pp. 20 et s.

appropriation en passant par des systèmes de propriété publique. Elle relève cependant que notre système juridique étant inconfortable avec la notion même de communauté, l'élaboration des droits et obligations à instituer autour d'une ressource liée à une communauté définie par un sentiment d'appartenance particulier s'avère délicate, et que plus délicate encore est la formulation d'une réponse juridique adéquate pour un phénomène proprement a-national comme internet.

La Commission estime toutefois qu'il est possible, **pour appréhender le phénomène des communs par notre droit,** de **se reporter à plusieurs instruments déjà opérationnels**.

Ainsi, la Commission rappelle la **possibilité de s'appuyer sur le régime dit des choses communes instauré à l'article 714 du code civil** et selon lequel « *il est des choses qui n'appartiennent à personne et dont l'usage est commun à tous* » et « *des lois de police règlent la manière d'en jouir* ».

Héritier des *Institutes* de Justinien qui, dès le VIe siècle, envisageaient les *res communis* du droit romain comme « *des choses qui sont par la loi de la nature communes au genre humain : l'air, l'eau des rivières, la mer et par conséquent le littoral des mers* » [(1)], l'article 714 du code civil vise également à instaurer la notion de choses communes. Mais si cette disposition a initialement été créée au vu de ces choses communes naturelles, rien n'empêche cependant, en adoptant une lecture normative [(2)], d'en élargir l'application non seulement aux choses communes par nature mais aussi aux choses communes par destination ou par affectation, telles que certains communs numériques. La notion de choses communes du code civil se caractérise par deux critères : la non-appropriation et l'usage ouvert à tous, en libre accès, sans cibler le bénéfice d'une communauté strictement délimitée. Certains juristes du XIXème siècle, comme Proudhon ou Duranton [(3)] évoquaient, à cet égard, l'institution de communautés « négatives » par refus de la propriété privée, permettant à tous d'avoir accès à la chose.

On reproche souvent à cette disposition son caractère potentiellement anarchique, lié à l'inorganisation des relations s'établissant sur la chose commune et ne permettant pas la gestion optimale de la ressource dans l'intérêt commun, ou encore les possibilités indirectes de réappropriation (par exemple par le dépôt d'une marque sur une œuvre qui ne serait plus protégée par le droit d'auteur). Cette absence de gouvernance serait également contraire à la qualification de communs au sens usuellement retenu pour ce terme, car le propre des communs

---

(1) Titre I du livre deuxième des Institutes *de Justinien.*

(2) M. Clément-Fontaine, « Le renouveau des biens communs : des biens matériels aux biens immatériels », op. cit. *: «* Aussi, selon une approche renouvelée de la notion de choses communes, l'article 714 est interprété comme ayant une valeur normative et non simplement descriptive d'un état des choses. Autrement dit, c'est parce qu'il y a une réelle volonté de laisser à l'usage commun certaines choses qu'elles sont qualifiées de choses communes et non en raison de leur nature. Celles-ci n'appartiennent à personne car il faut que l'usage soit commun à tous ».

(3) J.B.V. Proudhon, Traité du domaine de propriété et de la distinction des biens, *Bruxelles, 1842, p. 6 ; A. Duranton,* Cours de droit civil français suivant le code civil, *tome IV, Paris, 1844, p. 195.*

serait précisément l'existence de cette gouvernance à même de faire respecter l'usage partagé de la communauté [1].

La Commission estime toutefois que **les choses communes peuvent faire l'objet d'une régulation spontanée par des mécanismes de gouvernance communautaire d'une part**, et rappelle que **le second alinéa de l'article 714 du code civil prévoit expressément que « *des lois de police* » sont adoptées pour déterminer la manière de jouir de la chose commune d'autre part** [2]. Ainsi, rien n'empêche le législateur d'organiser les modalités de cette gouvernance et de se porter ainsi garant de la protection des communs.

La Commission considère qu'il est tout à fait envisageable que la reconnaissance des communs numériques puisse partiellement s'opérer *via* l'inclusion d'une ressource dans la catégorie des choses communes au sens de l'article 714 du code civil, si nécessaire en recourant à une loi de police.

Recommandation n° 93

La Commission estime qu'il est notamment possible de faire usage de l'article 714 du code civil afin de reconnaître une ressource en tant que commun numérique, en confiant à la puissance publique le rôle de garant de la jouissance commune, si nécessaire par une loi de police.

La Commission reconnaît cependant que cette disposition ne peut servir à appréhender l'ensemble des cas de figure relatifs aux communs. La difficulté vient notamment de ce que la loi française ne peut gouverner que ce qui ressort de son territoire et le rattachement d'un objet a-national comme internet au régime de l'article 714 du code civil serait de peu d'utilité, si un tel statut de chose commune n'était pas reconnu au niveau international. **Une réponse purement nationale n'apparaît pas adéquate, par exemple pour organiser la gouvernance du commun qu'est internet ou de certains communs transnationaux**.

À cet égard, la Commission exprime son **inquiétude quant au mode de gouvernance de l'internet par l'ICANN**, notamment au regard du manque de volonté des organes de l'institution de rendre compte (*accountability*) à la communauté internationale de la manière dont elle gouverne l'architecture d'adressage. Bien que le gouvernement américain ait finalement accepté d'abandonner la tutelle sur l'institution qui est une association de droit privé

---

(1) Y. Benkler, « Between Spanish Huertas and the Open Road : A Tale of Two Commons ? », Convening Cultural Commons Conference at NYU, *September 23-24 2011, p. 3 souligne que «* commons, including open access commons, almost never means lawlessness or anarchy (…). It means freedom-to-operate under symmetric constraints, available to an open, or undefined, class of users *».*

(2) Voir, sur ce sujet, M.-A. Chardeaux, Les choses communes, *préf. G. Loiseau, LGDJ, 2006, pp. 228 et s.*

américain, cette décision a fait l'objet d'un moratoire, faute pour l'ICANN de vouloir se soumettre à une autre forme de contrôle [1].

Ainsi le coût grandissant de l'obtention des nouvelles extensions de noms de domaine marque une évolution préoccupante vers une mercantilisation de l'accès à internet, de même que la précarité des droits des individus sur les noms de domaines qui leur sont attribués - notamment à travers des procédures unilatérales de retrait - démontre la fragilité des usages communs et l'absence de caractère démocratique de leur allocation. Par conséquent, **la Commission en appelle à une reconnaissance internationale positive d'internet comme un commun numérique dont la gouvernance par l'ICANN doit être assurée en conformité avec ce statut, à l'aide de la règle de la neutralité**.

À ce titre, et sans préjudice des autres instruments juridiques internationaux susceptibles d'être convoqués, la Commission considère que la **notion de patrimoine commun de l'humanité** [2], qui a notamment été utilisée à propos de l'Antarctique ou encore du génome humain, pourrait, en dépit de son actuelle faible effectivité [3], constituer une qualification opportune pour saisir internet comme un commun à l'échelle mondiale. L'institution chargée de la gouvernance de l'internet devrait être tenue de rendre compte de ses obligations d'accès universel et de gestion commune de cette ressource, notamment au regard d'un principe juridique de neutralité du réseau reconnu au plan international.

Recommandation n° 94

La Commission recommande de faire d'internet un commun au niveau mondial. La reconnaissance d'un statut de patrimoine commun de l'humanité pourrait être envisagée, sans exclure d'autres instruments juridiques internationaux. Les organes de gouvernance devront rendre compte de leur gestion commune de cette ressource, notamment au regard du principe de neutralité du réseau.

D'autres instruments de droit positif sont susceptibles d'être utilisés en droit français pour préserver des communs numériques. Sous propriété publique, le bien commun sera réglé selon le régime de la domanialité publique, en cas d'affectation à l'usage commun. Ce choix de privilégier une utilité collective de la ressource numérique peut se traduire par une politique volontariste de mise en partage des ressources publiques numériques et rejoint largement les préoccupations préalablement exprimées par la Commission dans le présent rapport d'**encourager l'*open data* pour les données publiques** (voir notamment

---

(1) *Voir* The Guardian, *« The internet is run by an unaccountable private company. This is a problem », 21 septembre 2015.*

(2) *Ch. Kiss, « La notion de patrimoine commun de l'humanité »,* Recueils des cours de l'Académie de droit international, *tome 175, vol. II, 1982, p. 103.*

(3) *Des propositions constructives existent, telle celle d'instituer un médiateur ou « ombudsman » pour les générations futures ou de généraliser la figure du* trust *de* Common Law *(cette technique permet précisément de faire gérer des ressources dans l'intérêt d'une communauté, bénéficiaire finale).*

recommandations n°s 4, 9 et 10 du présent rapport [1]) **tout en s'assurant que leur réutilisation ne permettra pas une réappropriation**.

Recommandation n° 95

La Commission réaffirme la nécessité d'encourager la préservation et l'enrichissement des communs numériques dans le cadre d'une politique volontariste d'*open data* des données publiques.

Enfin, les communs informationnels peuvent faire l'objet d'une combinaison de droits de propriété exclusive avec des règles d'usage partagés. Dans le domaine immatériel, cette cohabitation des droits exclusifs et des capacités d'usage s'établit en principe au sein des régimes de propriété intellectuelle lorsque l'objet est le siège de tels droits ou dans le cadre du domaine public informationnel lorsqu'aucune protection n'est reconnue.

S'agissant du **domaine public informationnel**, la Commission a déjà souligné qu'il ne faisait pas l'objet, à l'heure actuelle, d'une reconnaissance légale positive bien que son existence soit constamment établie par la doctrine juridique et que la jurisprudence ait déjà manifesté sa juridicité à travers certaines décisions refusant, par exemple, la réappropriation par un droit de propriété intellectuelle (une marque) d'un élément informationnel préalablement protégé par un autre droit de propriété intellectuelle mais dont la protection avait expiré (à propos de la protection de la forme d'une brique de *Lego*).

La Commission déplore toutefois qu'en l'absence de régime juridique précis, des **mécanismes directs ou indirects de réappropriation des éléments du domaine public informationnel** s'établissent soit par la mobilisation de droits de propriété intellectuelle, soit par la combinaison de dispositions contractuelles avec des mesures techniques de protection bloquant l'accès à une ressource numérique.

La Commission estime que la reconnaissance du domaine public informationnel doit être affirmée de manière positive [2], afin d'empêcher que des ressources numériques, dès lors qu'elles ont le statut de communs, ne fassent l'objet d'une exclusion d'usage.

Recommandation n° 96

La Commission estime que le domaine public informationnel doit faire l'objet d'une reconnaissance positive en droit français.

---

(1) Voir supra, *le* b *du 3 du A du I et les* a *et* b *du 2 du B du même I.*

(2) En ce sens, P. Lescure (dir.), Contribution aux politiques culturelles à l'ère numérique, *Rapport au ministre de la Culture et de la Communication, mai 2013, spéc. p. 448 et Fiche C-12. Pour des travaux scientifiques au support d'un tel régime, S. Dusollier,* Étude exploratoire sur le droit d'auteur et les droits connexes et le domaine public, *Rapport établi pour l'OMPI, avril 2010, spéc. p. 74.*

2. La conciliation des droits ou capacités d'usage et des droits de propriété intellectuelle

La Commission souhaite au préalable **réaffirmer l'importance du droit d'auteur pour les industries culturelles et le développement de la connaissance** et entend souligner la nécessité de préserver ou de renforcer les droits des créateurs et de ceux qui permettent le financement de la création. Elle dit en particulier son attachement au droit moral de l'auteur qui garantit son choix de communiquer l'œuvre au public, la paternité de l'œuvre et le droit à son respect et à son intégrité. Elle souligne que l'évolution des technologies et des usages crée de nouvelles relations entre les auteurs et interprètes et le public et a renforcé les pouvoirs de nouveaux acteurs industriels. Ces tendances invitent à une réflexion sur les adaptations du droit d'auteur à l'ère numérique, notamment des droits d'usage des œuvres numériques.

Relativement aux **mécanismes volontaires de mise à disposition ouverte des œuvres de l'esprit par leurs auteurs**, la Commission a pu dégager un point de vue convergent. Elle rappelle qu'il est possible de réaliser ***via* des licences libres** une mise en partage des œuvres qui s'apparente à un commun numérique « consenti » et qui offre aux utilisateurs des droits ou capacités d'usage étendues [(1)]. Elle **encourage leur pratique** et souligne, en principe, leur compatibilité avec le droit français et en particulier l'article L. 122-7-1 du code de la propriété intellectuelle qui dispose que « *l'auteur est libre de mettre ses œuvres gratuitement à la disposition du public, sous réserve des droits des éventuels coauteurs et de ceux des tiers ainsi que dans le respect des conventions qu'il a conclues* ». Elle appelle toutefois l'attention sur la **nécessité de lever les obstacles qui viennent limiter l'usage de ces licences libres**.

Recommandation n° 97

Encourager la pratique des mécanismes volontaires de mise à disposition ouverte des œuvres de l'esprit, notamment à travers des licences libres, en œuvrant à la levée des obstacles qui limitent leur usage.

La mise en jeu de la notion de communs à travers la revendication de l'exercice effectif de droits d'usage communs est susceptible de se heurter à la reconnaissance et à l'exercice des droits de propriété intellectuelle lorsque leurs titulaires souhaitent s'appuyer sur leurs droits exclusifs et suppose de trouver une juste conciliation entre ces deux prétentions légitimes.

Sur cette question, les membres de la Commission ne sont pas parvenus à un accord permettant d'énoncer une recommandation commune. Les éléments du débat peuvent ainsi être présentés :

---

(1) S. Dusollier, « The commons as a reverse intellectual property-from exclusivity to inclusivity », in H. R. Howe, J. Griffiths, Concepts of Property in Intellectual Property, *Cambridge, University Press, 2013, p. 265.*

a. Sur l'application du droit d'auteur à la sphère non marchande

Le débat public a vu naître, à travers notamment des travaux scientifiques et des déclarations politiques [(1)], **certaines revendications visant à reconsidérer l'application du droit d'auteur en tant que droit exclusif pour les activités non-marchandes** se déroulant par voie numérique. En raison de la difficulté matérielle à exercer un contrôle préalable sur des usages de masse mais aussi, et de manière plus fondamentale, pour permettre un partage de la culture et des connaissances entre individus, il serait instauré dans ce cas une **rémunération équitable** au profit des auteurs.

Les porteurs de ces revendications considèrent que, dans les années qui viennent, la délimitation d'une sphère de partage non-marchand entre individus des œuvres numériques sera une question politique clé. Ils estiment que cette délimitation est une condition de la reconnaissance du droit pour chacun de pratiquer ce partage, probablement en l'associant à la mise en place de nouveaux financements contributifs.

Constitue selon eux un partage entre individus toute transmission d'un fichier (par échange de supports, mise à disposition sur un blog ou sur un réseau pair à pair, envoi par email, etc.) d'un lieu de stockage « appartenant à l'individu » (ou « placé sous le contrôle souverain de l'individu ») à un lieu de stockage « appartenant à un autre individu ». Ils considèrent que cette notion recouvre aussi un espace de stockage sur un serveur, lorsque le contrôle de cet espace appartient à l'usager et à lui seul. Ils définissent le partage non-marchand comme le partage qui ne donne lieu à un aucun revenu, direct ou indirect (par exemple revenu publicitaire) pour aucune des deux parties. Le fait d'accéder gratuitement à un fichier représentant une œuvre qui fait par ailleurs l'objet d'un commerce ne constitue en aucun cas un revenu.

Dans ces conditions, ils défendent l'idée que si le partage non-marchand entre individus est légalisé, la fourniture de moyens à ce partage (par exemple opération d'un *hub DC++*, d'un serveur *eMule*, d'un indexer *BitTorrent*), sans centralisation des contenus numériques eux-mêmes et sans publicité associée à leur téléchargement ou à leur visionnement, écoute ou lecture doit pouvoir devenir légale, comme doit l'être la fourniture de moyens à une activité légale.

En définitive, ils envisagent le **partage non-marchand entre individus** à l'aune de **trois critères** : le **caractère non-marchand pour les individus parties** au partage, le **caractère décentralisé** (d'individu à individu) **de la transmission** de fichiers et l'**absence d'interférence d'un fournisseur de moyens commercial** avec les modalités du partage.

---

(1) *Blur-Banff proposal de 2002 ; Accord de Paris de 2006 ; William W. Fisher III,* Promises to keep : Technology, law, and the future of entertainment, *Stanford University Press, 2004 ; Philippe Aigrain,* Sharing : Culture and the Economy in the Internet Age, *Amsterdam University Press, 2012 ; Marco Ricolfi* Copyright 2.0.

Les **contradicteurs de cette thèse** font valoir, en premier lieu, que l'application du droit d'auteur, et notamment du droit moral, n'est pas distinguée selon que l'usage d'une œuvre protégée est faite dans un cadre « marchand » ou non. Ils soulignent, en second lieu, la **difficulté de déterminer ce qui relève de la sphère marchande et non-marchande** et les risques économiques afférents à cette difficulté pour les titulaires de droits. À cet égard, la frontière entre le « marchand et le « non-marchand » est ignorée dans le droit positif actuel et ne répond à aucune catégorie juridique identifiée.

L'absence d'intention lucrative et la gratuité initiale de l'échange, notamment dans le monde numérique, n'empêchent pas que ces échanges sont susceptibles, dans certains cas, de porter atteinte au marché de l'œuvre par la multiplication des sources d'accès et de reproduction qui constituent autant d'alternatives gratuites concurrentielles des modèles payants.

En outre, ils appellent l'attention sur le fait que l'exclusion pure et simple du droit exclusif d'auteur envers les individus qui opèrent des échanges constituerait un blanc-seing pour les plateformes qui sont utilisées pour opérer ces échanges et qui réalisent des profits à cette occasion.

Elles pourraient non seulement continuer à s'abriter, comme elles le font parfois indûment, derrière le statut d'hébergeur pour refuser tout assujettissement au système du droit d'auteur mais elles pourraient de surcroît se prévaloir de l'absence d'application du droit d'auteur en amont pour dénier toute implication dans le circuit d'exploitation. Une telle solution, sans un strict encadrement, mettrait irrémédiablement à terre toutes les tentatives des industries culturelles de faire payer aux plateformes le prix de la création dont elles tirent profit, à rebours des objectifs suivis par la France depuis plusieurs années.

Enfin, ils rappellent que les limitations ou exceptions au droit exclusif doivent répondre aux **exigences du triple test** selon lequel les limitations aux droits de propriété intellectuelle ne peuvent intervenir que dans des cas spéciaux, et ne doivent pas porter atteinte à l'exploitation normale de l'œuvre ni causer un préjudice injustifié aux intérêts légitimes de titulaires [(1)].

Dans ce contexte, il serait utile de poursuivre et d'approfondir le débat sur les avantages et inconvénients d'une reconnaissance du partage non-marchand décentralisé entre individus.

b. Sur la possibilité de reconnaître des droits culturels

Certaines propositions ont également été formulées dans un sens visant à dépasser la logique des exceptions aux droits de propriété intellectuelle pour conférer aux individus des droits culturels ou encore pour

---

(1) Article 9 de la Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886 ; article 13 de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce ; article 5 §5 de la directive 2001/29 sur les droits d'auteur et les droits voisins dans la société de l'information.

renforcer le champ des exceptions en faveur de la connaissance et du savoir, notamment en s'appuyant sur le rapport du Conseil des droits de l'homme dans le domaine des droits culturels des Nations unies intitulé *Politiques en matière de droit d'auteur et droit à la science et à la culture* (1) et celui de Mme Julia Reda au Parlement européen sur la révision de la directive de 2001 sur le droit d'auteur et les droits voisins dans la société de l'information (2).

Les membres de la Commission favorables à ces propositions se fondent sur les articles 27 de la Déclaration universelle des droits de l'homme du 10 décembre 1948 et 15 du Pacte international relatif aux droits économiques, sociaux et culturels du 16 décembre 1966 (3), qui ont pour trait commun de traiter ensemble les droits des auteurs et les droits de toute personne à participer à la vie culturelle de la cité et à l'avancement des connaissances.

Ils estiment que la reconnaissance de droits culturels de chacun à l'égard de toute œuvre n'est pas seulement une condition nécessaire pour l'existence d'une culture partagée mais aussi une condition pour que se développe une économie culturelle. Ils déplorent que, depuis une vingtaine d'années, certains acteurs des matériels, de la distribution, de l'édition ou de la gestion des droits aient mis en place des dispositifs techniques restreignant fortement l'usage des œuvres numériques en comparaison de celui des œuvres sur support non numérique et plus encore en comparaison de ce que ces droits devraient être pour réaliser le potentiel culturel de l'âge numérique. Ils relèvent que ces mêmes acteurs ont réclamé et obtenu des protections juridiques contre le contournement de ces dispositifs techniques, à l'instar des mesures techniques de protection, plus souvent appelées DRM (*digital rights management*) : d'abord pour la musique enregistrée avec les CD anti-copie et avec les fichiers avec DRM, puis pour l'image animée tout comme pour les livres numériques. Or, ils constatent qu'à chaque fois, le rejet par le public de cette régression des droits a considérablement fragilisé le marché des contenus correspondants et que c'est au moment même où *Apple* renonçait aux DRM que la France leur accordait une protection juridique si forte que même pour les besoins d'usages légaux, il n'était pas possible de s'en affranchir. Ils observent que le même processus est à l'œuvre aujourd'hui pour les livres numériques pour lesquels les éditeurs prennent conscience que l'imposition des DRM qu'ils ont au départ soutenue n'a fait que renforcer considérablement le pouvoir des fabricants de matériels qui sont en même temps distributeurs oligopolistiques (4). Ils font donc valoir que le marché a été conquis soit par les

---

(1) Rapport de la rapporteure spéciale dans le domaine des droits culturels, Farida Shaheed, Politiques en matière de droit d'auteur et droit à la science et à la culture, *février 2015, p. 1, qui recommande notamment* « d'accroître les exceptions et limitations au droit d'auteur afin de favoriser de nouvelles créations, de renforcer les avantages pour les auteurs, d'améliorer les possibilités d'éducation, de préserver le champ d'une culture non commerciale et de promouvoir l'intégration des œuvres culturelles et l'accès à celles-ci ».

(2) Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

(3) Le droit à l'éducation y a été également affirmé dans des termes forts aux articles 26 de la Déclaration universelle des droits de l'homme et 13 du Pacte des droits sociaux, économiques et culturels mais qui sont moins ouverts à une application spécifique à l'âge numérique.

(4) Apple *et* Amazon.

acteurs qui ont supprimé les DRM après avoir conquis une position dominante, soit surtout par les acteurs du *streaming* [1] et qu'il en est résulté une baisse de la part de la valeur ajoutée des auteurs et des éditeurs, dont seuls les distributeurs ont profité et, dans certains cas, des sociétés de gestion collective ayant passé des accords avec eux.

Pour contrer cette évolution néfaste, ils appellent à définir des droits d'usage minimaux de chacun à l'égard de toute œuvre numérique, quel que soit son mode de diffusion du moment et qu'elle soit rendue accessible au public sous forme numérique commercialement ou non. Ils estiment préférable que ces droits soient juridiquement reconnus comme droits culturels afin d'éviter tout retour en arrière à l'occasion d'un changement technique ou en raison de l'intérêt d'un acteur [2], ce qui n'interdit pas d'admettre des exceptions et des limitations à ces droits culturels. Toutefois, ils souhaitent que soit clairement précisé que ces exceptions et limitations ne sauraient avoir pour effet de limiter les droits d'usage, y compris pour les créateurs de nouvelles œuvres qui en ont besoin bien au-delà du seul champ du *remix* ou *mashup*.

En somme, les membres de la Commission favorables à cette position recommanderaient de définir des droits d'usage minimaux de chacun à l'égard des œuvres numériques en les instituant en droits culturels.

Ils considèrent que cette approche pourrait se concrétiser par l'adoption de dispositions nationales sans changement du droit communautaire applicable, s'inscrivant dans quatre directions : l'adoption ou le renforcement des exceptions essentielles au droit d'auteur constitutives de droits d'usage (droit de citation s'appliquant à tous les médias, exception pour l'éducation et la recherche, exceptions de parodie et satire, exception d'interopérabilité, etc.) ; l'affirmation que les droits d'usage reconnus seront effectifs à l'égard de tout dispositif technique, la protection de ces dispositifs contre le contournement ne pouvant pas être invoquée lorsque le dispositif technique fait obstacle à un droit d'usage reconnu ; la création d'un droit à l'opérabilité auquel la protection contre le contournement des mesures techniques de protection ne puisse être opposée, un tel droit étant le seul moyen de combattre efficacement les monopoles et les oligopoles des fabricants de matériels intégrés verticalement avec la distribution et des fournisseurs de systèmes d'exploitation des dispositifs numériques ; enfin, la reconnaissance du droit pour les bibliothèques, centres d'archives ou organismes d'éducation artistique et culturelle à faire bénéficier dans leurs locaux ou sur internet leurs usagers des droits d'usage qui leur sont reconnus comme individus.

En définitive, les membres de la Commission favorables à cette position recommanderaient, à droit communautaire constant, de définir les exceptions

---

(1) Spotify, YouTube, Netflix.

(2) Ce fut le cas par exemple lorsque l'exception pour copie privée, qui était clairement entendue par le législateur de 1985 comme un droit de chacun, fut soudain redéfinie comme une tolérance temporaire susceptible d'être supprimée au prétexte qu'il serait possible d'empêcher par un moyen technique de l'exercer.

essentielles au droit d'auteur constitutives de droits d'usage, de renforcer l'effectivité de ces droits à l'égard de tout dispositif technique, de créer un droit à l'opérabilité et de reconnaître le droit pour les bibliothèques, les centres d'archives ou les organismes d'éducation artistique et culturelle à faire bénéficier dans leurs locaux ou sur internet leurs usagers des droits d'usage qui leur sont reconnus comme individus.

En réponse à ces propositions, plusieurs membres de la Commission ont souligné que la reconnaissance constitutionnelle des droits de propriété intellectuelle en tant que droits de propriété a conduit, jusqu'à présent, la jurisprudence tant française qu'européenne à **interpréter de manière restrictive les exceptions au droit d'auteur et à leur refuser la qualité de droit subjectif** (1).

Ils estiment en outre que **le régime juridique existant d'exceptions au droit d'auteur garantit d'ores et déjà une multiplicité d'usages des œuvres**, notamment en matière d'enseignement et de recherche, d'archivage, de conservation et d'accès en bibliothèque ou encore de citation et de parodie. Ils font remarquer, à cet égard, que la loi française a opéré depuis plusieurs années des évolutions majeures sur ces différents points. Alors qu'aucune exception n'existait à propos de l'enseignement et de la recherche ou des bibliothèques depuis la création du droit d'auteur en France, le législateur en a introduit dans la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI), des exceptions qui ont sans cesse été élargies par les lois postérieures. Ainsi, ces membres considèrent que la législation française, tout comme le droit européen, ont, ces dix dernières années, constamment étoffé les capacités légales d'usage en renforçant le nombre et l'étendue des exceptions, notamment à l'ère numérique.

En outre, ils mettent en garde contre une représentation erronée consistant à **confondre le contrôle technique des exploitations des œuvres par les titulaires de droits, considéré comme légitime** au regard des traités de l'Organisation mondiale de la propriété intellectuelle (OMPI) de 1996 et de la directive 2001/29 du 22 mai 2001 dite « Infosoc », **et le contrôle d'accès décidé de manière unilatérale par les plateformes de distribution et opposable aux utilisateurs qui ont signé les conditions générales d'utilisation dans lesquelles un tel contrôle est prévu**. Ces pratiques se font le plus souvent en marge du droit d'auteur, voire à l'encontre de l'intérêt des titulaires de droits qui n'ont d'autre choix que de les accepter s'ils veulent voir leurs œuvres diffusées sur internet.

Ainsi, pour garantir le respect effectif des exceptions, il conviendrait de préciser dans la loi qu'elles sont, pour l'ensemble ou certaines d'entre elles, d'ordre public. Il conviendrait, en outre, d'empêcher que les plateformes de distribution oligopolistiques n'imposent leurs modèles de contrôle d'accès au

---

(1) En droit français, voir notamment les décisions de la Cour de cassation dans l'affaire Mulholland Drive *où les juges ont refusé de reconnaître à l'exception de copie privée le statut de droit à la copie privée.*

détriment de l'exercice du droit des auteurs et des capacités légales d'usage des utilisateurs reconnues par les exceptions.

S'agissant du droit à l'interopérabilité, ils soulignent qu'**un dispositif *ad hoc* a déjà été mis en place devant la HADOPI** pour permettre une certaine interopérabilité, regrettent que ce mécanisme n'ait pas connu un succès suffisant (1) et invitent à le reconsidérer pour garantir son effectivité tout en indiquant que le droit de la concurrence a d'ores et déjà été mis à profit pour favoriser l'interopérabilité. Ils rappellent qu'une tentative d'instaurer un tel droit a déjà fait l'objet d'une censure par le Conseil constitutionnel en raison du caractère trop imprécis de son intitulé et qu'il conviendrait, par conséquent, de le délimiter plus clairement, conformément aux indications fournies par la Cour de Justice de l'Union européenne dans l'affaire *Nintendo* (2).

Enfin, **s'agissant de la possibilité de bénéficier d'une exception lorsque la diffusion de l'œuvre est organisée *via* des DRM déterminés par les titulaires**, ces membres font valoir que si, dans l'affaire *Mulholland Drive* (3), **la Cour de cassation** a refusé la possibilité de se prévaloir devant le juge judiciaire d'un droit à la copie privée pour forcer le déblocage d'un DRM sur une œuvre, elle **n'a pas exclu**, en revanche, **d'actionner le bénéfice d'une exception pour justifier le contournement d'une mesure technique de protection qui en empêcherait la jouissance**. Ils font valoir, en outre, qu'une possibilité d'invocation positive d'une exception contre un DRM existe devant la HADOPI et regrettent que le mécanisme n'ait pas donné lieu à des résultats probants en raison notamment du caractère dissuasif de la procédure. Ils appellent par conséquent à **reconsidérer le dispositif de conciliation de manière à garantir le bénéfice effectif des exceptions**, conformément à l'article 6 § 4 de la directive 2001/29 précitée, voire à **reconsidérer l'élargissement de ce mécanisme de préservation des usages à de nouvelles exceptions et à d'autres formes de distribution** que celles qui sont visées dans ledit texte.

3. Renforcer les droits des créateurs au titre de l'exploitation numérique de leurs œuvres et favoriser des modèles de rémunération équitable

Le bouleversement rapide des modes de consommation et des modèles d'affaires induit par le numérique, marqué en particulier par l'émergence de nouveaux intermédiaires (services de *streaming* et de téléchargement, plateformes de vidéo à la demande, magasins de livres numériques, etc.), suscite de fortes tensions sur le « partage de la valeur » entre, d'une part, les créateurs et leurs éditeurs ou leurs producteurs et, d'autre part, les titulaires de droits et les plateformes.

---

(1) La HADOPI a fait l'objet essentiellement d'une saisine à ce propos dans l'avis dit VLC dans lequel elle a poussé les parties à trouver un accord et a refusé d'ordonner à Sony de délivrer les informations essentielles à l'interopérabilité.

(2) CJUE, 23 janvier 2014, Nintendo c. PC Box & 9Net, *n° C-355/12.*

(3) Cass. 1ère civ., 28 février 2006, n° 05-15.824 et 19 juin 2008, n° 07-14.277.

Comme l'indique le rapport remis par M. Pierre Lescure en mai 2013 sur l'acte II de l'exception culturelle [(1)], « *les rapports entre ceux qui créent ou produisent les œuvres et ceux qui assurent leur diffusion ou leur distribution en ligne restent globalement difficiles. Ces tensions s'expliquent à la fois par la diminution générale des prix unitaires qui a accompagné la dématérialisation des biens culturels et par l'émergence de nouvelles formes d'exploitation inconnues dans l'univers analogique. Ces modèles d'affaires, qui ne sont pas encore stabilisés, bouleversent les conditions traditionnelles de partage de la valeur et suscitent des incompréhensions* ». Le rapport souligne à cet égard que « ***les conditions de rémunération des créateurs (auteurs et artistes) tardent à s'adapter à l'évolution des modes d'exploitation des œuvres*** » [(2)].

La question du partage de la valeur liée à l'exploitation en ligne des œuvres se pose avec une acuité particulière **dans le secteur de la musique**. Les artistes-interprètes contestent en particulier les modalités du partage de la valeur créée par l'exploitation de la musique en ligne. Ils soulignent l'opacité des modalités de calcul (notamment de l'assiette et des abattements pratiqués par les producteurs) et la faiblesse des rémunérations unitaires attachées aux actes de téléchargement ou d'écoute en *streaming*, ces revenus étant notamment rapportés tant à ceux obtenus pour les exploitations physiques qu'à ceux qui résulteraient d'un partage paritaire comparable à celui des licences légales.

Le projet de loi relatif à la liberté de la création, à l'architecture et au patrimoine, en cours d'examen au Parlement au moment de la préparation du présent rapport, tend à apporter de premières réponses à travers des dispositions destinées à améliorer la position contractuelle des artistes-interprètes, l'institution d'un médiateur de la musique chargé de réguler les relations entre artistes-interprètes, producteurs et plateformes et l'encadrement par la loi d'une négociation destinée à fixer une garantie de rémunération minimale en faveur des artistes-interprètes pour l'exploitation de leur prestation en *streaming*.

S'agissant du livre numérique, le rapport « Lescure » observe que « *les pourcentages reversés par les éditeurs aux auteurs sont, en règle générale, légèrement plus élevés que pour le livre imprimé ; toutefois, compte tenu de la différence de prix, ces pourcentages se traduisent par une rémunération à l'acte plus faible en valeur absolue. En outre,* ***la rémunération des auteurs au titre des nouveaux modèles d'exploitation*** *(offre de « bouquets de livres », location, modèles gratuites financés par la publicité, vente de livres au chapitre, etc.)* ***soulève de nombreuses interrogations*** » [(3)].

L'ordonnance n° 2014-1348 du 12 novembre 2014 modifiant les dispositions du code de la propriété intellectuelle relatives au contrat d'édition a transposé les grands principes qui ont fait l'objet de l'accord-cadre du

---

(1) Pierre Lescure, Mission « Acte II de l'exception culturelle », Contribution aux politiques culturelles à l'ère numérique, *mai 2013, p. 19.*

(2) Pierre Lescure, op. cit., *p. 20.*

(3) Pierre Lescure, op. cit., *p. 20.*

21 mars 2013, issu d'un long et difficile processus de négociation interprofessionnelle sur l'évolution du contrat d'édition à l'ère numérique, entamé dès 2007 entre le Conseil permanent des écrivains (CPE) et le Syndicat national de l'édition (SNE). Si les réflexions ont largement porté sur l'adaptation des règles aux nouveaux modes d'exploitation numérique, elles ont également permis de préciser l'application de certaines règles essentielles à l'édition imprimée, s'agissant par exemple des modalités de reddition des comptes ou de l'étendue de l'obligation pesant sur l'éditeur en matière d'exploitation permanente et suivie. Si ces dispositions ont eu pour objet d'améliorer l'équilibre des relations entre auteurs et éditeurs, **il peut paraître nécessaire d'aller encore plus loin dans le rééquilibrage de ces relations**.

Recommandation n° 98

Garantir aux auteurs et aux artistes un intéressement juste et équitable aux fruits de l'exploitation numérique de leurs œuvres, en intégrant notamment les économies liées à la production et à la diffusion numériques dans les assiettes et les taux des rémunérations qui leur sont dues.

4. Approfondir le droit à l'exploitation et au partage des connaissances scientifiques : le libre accès (*open access*)

Le numérique transforme en profondeur les modes de production et de diffusion des résultats scientifiques : données, publications, analyses sont désormais potentiellement universellement et immédiatement accessibles en ligne, sur des plateformes. Cette disponibilité potentielle du matériau scientifique recèle une promesse inouïe d'exploitation et de partage des connaissances et vient réinterroger l'équilibre actuel du régime de la publication scientifique. La recherche d'intérêt général financée sur fonds publics se doit d'être à la pointe de cette évolution. Dans ce contexte, il est proposé de faire évoluer les droits respectifs du chercheur publiant, de son institution de rattachement et de ses lecteurs – humains ou mécaniques – ainsi que des intermédiaires spécialisés dans la rencontre entre ces acteurs – les revues et les éditeurs scientifiques, dans le cas de recherches financées majoritairement par des fonds publics.

L'information scientifique ne bénéficiant pas d'un statut juridique particulier qui la distinguerait d'autres formes d'informations, les études et travaux issus de la recherche scientifique sont appréhendés comme des œuvres écrites, à ce titre susceptibles d'être protégées par le droit d'auteur. Or, de par la nature même de leur activité, les chercheurs des organismes de recherche publics publient les résultats de leurs recherches dans des revues et sont amenés à opérer une cession des droits d'auteurs au profit des éditeurs. Les paramètres de ce transfert dans un monde non-numérique se révèlent moins bien adaptés à la circulation accélérée des informations dans le monde numérique : cessions exclusives trop longues, droits de reproduction et de diffusion trop limités.

Faciliter et accélérer cette circulation revêt aujourd'hui un caractère stratégique pour la recherche publique française : ce qui n'est pas accessible facilement et très vite a peu de chances d'être jamais lu, moins encore de compter, dans un monde où la compétition entre les chercheurs et les institutions est plus âpre que jamais.

Il s'ensuit plusieurs situations pénalisantes pour la communauté scientifique publique et, parce que ces résultats d'intérêt général sous-tendent l'ensemble des activités de recherche appliquée et d'innovation dans les entreprises, un manque à gagner pour l'économie française et des opportunités manquées de densification des relations entre recherche publique et entreprises.

Premièrement, en plus de céder tous leurs droits sur leurs écrits, les chercheurs académiques et les organismes publics de recherche dont ils dépendent sont le plus souvent soumis à un double paiement, puisqu'ils doivent à la fois assumer les frais de publication en amont et les frais de consultation en aval [(1)]. Il s'agit d'un poids important, tant pour les finances publiques que pour la productivité de la recherche publique qui est déjà fortement concurrencée au niveau international. Ce jeu des mécanismes de la propriété intellectuelle et des conventions aboutit à une captation de l'information scientifique au détriment des institutions publiques, qui ont un accès payant et restreint aux connaissances issues des programmes de travaux qu'elles financent. Il existe par ailleurs un déséquilibre important entre les organismes de recherche et les éditeurs, aggravé par l'émergence, ces dernières années, d'oligopoles de fait dans le secteur de l'édition scientifique (*Elsevier*, *Springer*, *Wiley*…).

C'est sur la base de ce constat que s'est construit le mouvement en faveur du libre accès (*open access*) [(2)] qui vise à desserrer la pression des coûts de publication sur les budgets des établissements publics et, surtout, à faciliter l'accès des connaissances scientifiques pour la communauté académique, mais aussi pour la société civile et les acteurs économiques (notamment les petites et moyennes entreprises) et dans le même temps à renforcer leurs capacités d'innovation. En 2012, la Commission européenne invitait en ce sens les États membres à « *définir des politiques claires en matière de diffusion des publications scientifiques issues*

---

(1) Les établissements d'enseignement supérieur et de recherche dépensent ainsi annuellement plus de 80 millions d'euros pour avoir accès à ces ressources en ligne, et les prix d'accès augmentent continuellement (plus de 7 % par an depuis 10 ans).

(2) Selon la déclaration de Béthesda de 2004, une publication en libre accès doit remplir deux conditions : « 1) Le/les auteur(s) ainsi que les titulaires du droit d'auteur accordent à tous les utilisateurs un droit d'accès gratuit, irrévocable, mondial et perpétuel et leur concèdent une licence leur permettant de copier, utiliser, distribuer, transmettre et visualiser publiquement l'œuvre et d'utiliser cette œuvre pour la réalisation et la distribution d'œuvres dérivées, sous quelque format électronique que ce soit et dans un but raisonnable, et ce à condition d'en indiquer correctement l'auteur ; ils accordent également aux utilisateurs le droit de faire un petit nombre de copies papier pour leur usage personnel. 2) La version complète de l'œuvre, ainsi que tout document connexe, dont une copie de l'autorisation ci-dessus, réalisée dans un format électronique standard approprié, est déposée dès sa publication initiale dans au moins un réservoir en ligne subventionné par un établissement d'enseignement supérieur, une société savante, une agence gouvernementale ou tout autre organisme reconnu œuvrant pour le libre accès, la diffusion sans restriction, l'interopérabilité, et l'archivage à long terme ».

de la recherche financée par des fonds publics et du libre accès à ces dernières » [1].

Dès lors, la Commission est d'avis d'**adapter le cadre législatif afin d'encourager ce mouvement**.

Il s'agit, en premier lieu, de **reconnaître à l'auteur un droit à l'« exploitation secondaire »** de ses écrits scientifiques financés majoritairement par des fonds publics, afin que la version de l'auteur déposée dans une archive institutionnelle reste en accès libre, quelles que soient les suites éditoriales données à ces travaux. Un tel maintien en ligne de la dernière version de travail soumise à la revue pour publication (*pre-print*) correspond d'ailleurs déjà à la pratique informelle de nombreuses communautés scientifiques, qu'une évolution du droit viendrait consolider et étendre.

Recommandations n° 99

Reconnaître à l'auteur un droit à l'exploitation secondaire, afin que la version de l'auteur déposée dans une archive institutionnelle reste en accès libre quelles que soient les suites éditoriales données à ces travaux.

En second lieu, il paraîtrait utile, à l'image du droit allemand, de **rendre librement accessibles les publications scientifiques financées majoritairement sur fonds publics**, après une durée d'exclusivité qui soit suffisamment longue pour maintenir l'équilibre économique de revues numériques, et suffisamment courte pour élargir de manière significative l'audience ayant accès à l'article dans sa version en accès libre ; les travaux académiques et les comparaisons avec les pratiques internationales conduisent à une durée recommandée de 6 à 12 mois.[2]

Afin de rendre effectif le droit exposé ci-dessus, obligation pourrait être faite, s'agissant de travaux de recherche financés sur fonds publics, d'une publication accessible gratuitement en ligne après le délai d'exclusivité déjà évoqué (sur site institutionnel, dans une revue ouverte, sur un site d'archive ou par ouverture automatique par la revue elle-même). Il est important toutefois que cette obligation ne repose pas sur les chercheurs eux-mêmes, mais plutôt sur les organismes de recherche, et nécessaire qu'elle soit précédée, domaine académique par domaine académique, d'une analyse des dynamiques économiques propres à chaque discipline [3].

---

(1) Recommandation de la Commission du 17 juillet 2012 relative à l'accès aux informations scientifiques et à leur conservation (2012/417/UE).

(2) Maya Bacache-Beauvallet, Françoise Benhamou, Marc Bourreau, « Quelle politique de libre accès pour les revues de sciences sociales en France ? », Rapport de l'Institut des politiques publiques n°19, juillet 2015.

(3) Il faut noter que les travaux effectués dans le cadre autorisé des activités extérieures des agents publics échapperaient naturellement à une telle obligation (cas des manuels, par exemple).

Enfin, les pouvoirs publics pourraient **encourager les chercheurs à mettre en accès libre les données brutes et anonymisées de la recherche**, à chaque fois que cela ne se heurte pas à des questions déontologiques ou de vie privée.

Recommandation n° 100

Rendre librement accessibles les publications scientifiques financées sur fonds publics, après un délai d'exclusivité limité à quelques mois permettant l'activité commerciale de l'éditeur.

Encourager les chercheurs à mettre en accès libre les données brutes et anonymisées de la recherche, à chaque fois que cela ne se heurte pas à des questions déontologiques ou de vie privée.

SOMMAIRE DES ANNEXES

I – Remise du rapport à M. Claude Bartolone, Président de l'Assemblée nationale 253

A – Intervention de M. Claude Bartolone, président de l'Assemblée nationale 253

B – Intervention de M. Christian Paul, député de la Nièvre, co-président.....256

C – Intervention de Mme Christiane Féral-Schuhl, avocate spécialiste de l'informatique et des nouvelles technologiques, ancienne bâtonnière de Paris, co-présidente 260

II – Déclarations 265

A – Déclaration de Mmes les députées Virginie Duby-Muller et Laure de la Raudière, et de MM. les députés Franck Riester et Patrice Verchère 265

B – Déclaration de MM. Philippe Aigrain et Edwy Plenel : une avancée importante pour le droit de savoir et une occasion manquée pour les droits culturels 265

III – Contributions au groupe de travail sur la vie privée 273

A – Contribution de M. Winston Maxwell : la notion de consentement.....273

B – Contribution de M. Daniel Le Métayer : analyser et prévenir les risques d'atteinte à la vie privée 276

C – Contribution de Mme Francesca Musiani : la notion de *privacy by design* 282

D – Contribution de M. Cyril Zimmermann : la notion d'*accountability*.....286

IV – Liste des 100 recommandations.....291

V – Liste des personnalités auditionnées.....307

VI – Liste des personnes rencontrées à Bruxelles 309

I. REMISE DU RAPPORT À M. CLAUDE BARTOLONE, PRÉSIDENT DE L'ASSEMBLÉE NATIONALE

A. INTERVENTION DE M. CLAUDE BARTOLONE, PRÉSIDENT DE L'ASSEMBLÉE NATIONALE

Monsieur le Président de la commission des affaires culturelles et de l'éducation, cher Patrick Bloche,

Madame la Présidente de la commission de réflexion, chère Christiane Féral-Schuhl,

Monsieur le Président de la commission de réflexion, cher Christian Paul,

Mesdames et messieurs les députés, chers collègues,

Mesdames et messieurs les personnalités qualifiées,

Mesdames, Messieurs,

« *La révolution numérique va de pair avec celle qui se donne à voir en matière juridique, où l'idéal d'une gouvernance des nombres tend à supplanter celui du gouvernement par les lois* ».

Votre rapport est une forme de réponse à la terrible alerte lancée par le professeur au collège de France Alain Supiot.

Il est la preuve que rien n'est joué d'avance et que si le « *combat pluriséculaire qui oppose émancipation et domination* », comme vous l'écrivez, a trouvé un nouveau domaine de lutte, nul ne peut pour l'instant en prédire l'issue.

Car si la révolution numérique présente bien des dangers, elle est surtout porteuse d'espoirs et de libertés.

Dès la première phrase de votre rapport vous le rappelez : «*toute révolution industrielle appelle un nouvel âge démocratique* ».

Je ne peux que partager ce constat.

Et cela alors que nous venons de présenter, ici même, il y a moins d'une semaine, avec l'historien Michel Winock, un rapport intitulé « *Refaire la démocratie* », qui se veut être, non un programme, mais une invitation adressée au citoyen.

Car oui nous devons penser ce que sera demain notre démocratie. Ce que seront demain nos libertés et notre droit.

Lors de la réunion d'installation de votre commission, il y a de cela 18 mois, nous disions ensemble à quel point il était nécessaire de définir une démarche globale, une approche commune, une doctrine et des principes durables en matière de protection des droits et libertés à l'âge numérique.

Les récents débats parlementaires ont souligné, ô combien, la pertinence de ce constat.

Votre rapport est, à ce titre, remarquable.

Sur la forme, tout d'abord, vous avez su, élus et membres de la société civile, députés de la majorité et de l'opposition, travailler ensemble, et mener une véritable réflexion. Cela ne fait que confirmer, selon moi, à quel point c'est en s'ouvrant sur l'extérieur, que le Parlement pourra assumer son rôle d'animation du débat démocratique.

Je tiens à remercier vivement tous les membres de la commission.

Je remercie particulièrement Maître Christiane Féral-Schuhl, qui a accepté d'en assumer la coprésidence, et qui a su apporter toute son expertise du secteur du droit de l'informatique et des nouvelles technologies.

Je remercie évidemment Christian Paul, qui m'a proposé la création de cette commission.

Dans ce magnifique récit qu'est la Bible, David vainquit le géant Goliath avec une fronde. Je ne sais pas si ce rapport est une fronde permettant de combattre de nouveaux Goliaths numériques, mais je sais ce qu'il doit au travail et à la rigueur intellectuelle de son coprésident.

Comment ne pas remercier également le remarquable travail des administrateurs, dont on ne louera jamais assez la disponibilité, la qualité, et la discrétion.

Remarquable, il l'est également en raison des 25 auditions que vous avez su mener, de la qualité de vos échanges avec le Conseil national du numérique, et du dialogue que vous avez réussi à nouer avec les instances communautaires.

Vous avez également travaillé de façon étroite avec la Chambre des députés italienne – je peux en témoigner – à l'élaboration d'une déclaration commune sur les droits et devoirs numériques du citoyen, que j'ai signée le 28 septembre dernier avec mon homologue et amie Laura BOLDRINI.

Remarquable sur la forme, votre travail l'est également sur le fond. Je ne saurais évidemment résumer ici vos 100 propositions. J'aimerais néanmoins insister sur un ou deux passages du rapport qui m'ont particulièrement intéressé.

D'abord, votre attachement à la loi de 1881 sur la liberté de la presse qui doit être préservée et renommée « loi sur la liberté d'expression », ainsi que votre

volonté de voir la place du juge, comme garant de la liberté d'expression, réaffirmée et consolidée. Je partage pleinement cette idée.

Votre souhait, ensuite, de voir reconnu et assuré un véritable droit à l'autodétermination du citoyen sur ses données personnelles. Je pense en particulier à vos réflexions sur la notion de consentement, concept qui nous interroge tous, en tant qu'utilisateur d'outils numériques.

J'ai été, à ce titre, également extrêmement intéressé par vos développements sur le droit au déréférencement qui, s'il doit être réel, doit être nécessairement encadré.

Enfin, je souligne et fais mienne votre proposition de nommer une personnalité indépendante, chargée de protéger les lanceurs d'alerte contre d'éventuelles menaces. Ils sont en effet les garants du contrôle démocratique, et leur action doit plus que jamais être protégée.

Au fond, seule la partie V de votre rapport, et la question des droits d'auteurs, continue à vous diviser. Ce sujet est effectivement extrêmement complexe.

Pour ma part, j'estime qu'il ne peut être résolu sans un véritable débat avec l'ensemble des acteurs, et en particulier avec les auteurs, et le monde de la culture. Cette partie est donc un peu à part. Je note d'ailleurs que vous n'y avez formulé aucune proposition commune.

***

À la lecture de votre travail, on le comprend bien : nous ne sommes qu'au début du chemin. La route sera encore longue avant que l'Assemblée nationale ne maîtrise pleinement les enjeux liés à ces questions.

Une chose est sûre : votre rapport contribuera à l'éclairer.

Il ne sera pas à lui seul suffisant, c'est évident. Nous l'avons bien vu au moment où vous avez émis votre avis sur le projet de loi relatif au renseignement.

Pour autant, nulle loi n'est immuable : ce qui a été fait un jour – et dans un contexte particulier – devra nécessairement être, à l'avenir, évalué et repensé.

En attendant, nous devons poursuivre ce travail d'acculturation aux enjeux du numérique. Dans cette perspective, nous devrons nous demander comment ceux-ci peuvent être mieux appréhendés dans le cadre de la procédure législative.

Mais en attendant, ne désespérons pas : le *« gouvernement par les lois »* peut encore gagner !

Je vous remercie.

B. INTERVENTION DE M. CHRISTIAN PAUL, DÉPUTÉ DE LA NIÈVRE, CO-PRÉSIDENT

Monsieur le Président,

Madame la co-présidente,

Mesdames, messieurs,

Mardi matin, sur la plainte d'un jeune autrichien de 27 ans, Max Schrems, la Cour de justice de l'Union européenne a annulé l'accord dit *« Safe Harbor »*. Cet accord encadrait le transfert vers les Etats-Unis par les entreprises américaines, Facebook en tête, des données personnelles des citoyens européens qui utilisent leurs services.

La Cour a considéré que les programmes de surveillance massive des Etats-Unis ne sont pas compatibles avec la protection des droits des citoyens européens.

C'est un événement mondial. Il confirme **l'actualité et l'âpreté du combat pour les libertés numériques**, déjà illustré par l'engagement d'Edward Snowden, dont je redis ici qu'il devrait avoir asile et protection sur le territoire français. Désormais, un homme seul comme Max Schrems peut se dresser devant les géants du capitalisme informationnel, et gagner la partie.

Cet événement fait écho à la bataille d'idées que cette commission a souhaité conduire. Il marque aussi la transformation de notre démocratie.

Ce nouvel âge démocratique est au cœur de nos travaux. Il en est le fil conducteur.

Nous faisons le pari que dans un monde déserté par tant d'utopies, **il y a encore de la place pour l'extension des droits et le progrès des libertés.**

C'est la démonstration que le progrès ne s'arrête pas. Il prend simplement d'autres formes.

Nous savons aussi que dans ce nouveau monde, **le droit qui protège est plus que jamais nécessaire.**

Nous faisons **le pari optimiste du numérique**, quand d'autres s'enferment dans le « blues technologique », et quand d'autres encore diabolisent le numérique.

De ce point de vue, la période récente n'a pas réservé que de bonnes surprises dans notre pays. L'activité législative, jusqu'ici, s'est faite contre l'avis de tous les acteurs du numérique rassemblés. Nous l'avons vécu en direct avec la

loi relative au Renseignement. **Cette loi n'a pas échappé à la tentation de la surveillance de masse par les algorithmes**. Malgré nos recommandations unanimes.

Mais il y a en France heureusement de puissants foyers d'optimisme. Dans la jeunesse, dans l'économie numérique qui décolle dans une incroyable créativité.

Dans le travail d'institutions comme la CNIL, l'ARCEP, le Conseil national du Numérique. Mais aussi le Conseil d'Etat. Beaucoup convergent. C'est un signal qu'il faut amplifier.

Avant d'en venir plus au fond, je veux d'emblée rendre **un double hommage**. D'abord aux membres de cette commission atypique que vous avez voulue, monsieur le président, avec une composition qui transgresse les figures imposées du Parlement.

Treize parlementaires, et treize acteurs et experts du monde numérique. Les seconds ne furent pas les moins assidus.

Ce rapport a été élaboré dans un esprit qui dépasse les clivages habituels. **Les 100 recommandations ont été adoptées à l'unanimité** à une ou deux exceptions. Quand des divergences sont apparues, j'y reviendrai, nous avons eu à cœur d'approfondir les positions et de circonscrire les désaccords, en évitant qu'ils soient artificiels. C'est là aussi une petite gorgée de démocratie.

Un second hommage s'adresse à une exceptionnelle équipe d'administrateurs qui nous a accompagnés sans relâche depuis 18 mois. Leur compétence et leur appétence pour les sujets les plus complexes ont fait des miracles.

Je veux **vous rendre compte de nos travaux, et le faire à deux voix avec Christiane Féral-Shuhl**, infatigable et exigeante co-présidente de notre commission.

À l'arrivée, ce rapport offre ***un manifeste de la démocratie* dans la société numérisée**. Nous sommes confrontés à des questions qui émergent très vite, comme dans les moments de changements et de ruptures, où les mutations de la société appellent des choix politiques.

Les périodes de rupture, comme 1789, la révolution industrielle, les débuts de la Troisième République, ou 1945 : à chaque fois la France vit des transitions entre l'ancien et le nouveau, des conflits d'intérêt, des confrontations vigoureuses.

De là, naissent des droits et des libertés, un nouvel écosystème démocratiques. Nous sommes très exactement dans un de ces moments, la guerre civile en moins, et l'Europe en plus.

Je mettrai brièvement en lumière **trois thèmes essentiels** de ce rapport, renvoyant chacun à une lecture plus complète de ce rapport.

1) L'approfondissement grâce au numérique d'un principe démocratique hérité des Lumières, des grandes lois de la Troisième République : **le droit de savoir. Ce droit, nous devons le fortifier.**

Il est contemporain de la dématérialisation, et de l'*open data*.

C'est un droit d'accéder à toute l'information d'intérêt public, qui devient la règle et non l'exception. Non seulement pour la presse, mais pour tous les citoyens.

2) La consécration progressive de **droits et de libertés nés avec la société en réseau et le numérique**. Ces libertés sont *digital natives*.

Nous en avons affirmé trois :

- **le droit d'accès à internet** : ce principe est déjà dans le bloc de constitutionnalité depuis la décision Hadopi du Conseil constitutionnel. Nous proposons de le renforcer.

- **la neutralité des réseaux** est un principe vital pour l'avenir des réseaux, pour la liberté d'expression, mais plus généralement, pour éviter une privatisation de l'internet. Nous proposons de consacrer ce principe, et à titre personnel, je considère qu'il pourrait trouver sa place dans notre constitution. Il a dans la civilisation numérique la force du principe d'égalité dans le débat républicain.

- **la loyauté des plateformes** : c'est l'exigence la plus récente, celle du respect des grandes plateformes à l'égard de leurs utilisateurs. Il fallait sans retard clarifier son contenu, fait de transparence et de non-discrimination. Elle incarne la dualité du monde numérique. Les algorithmes servent la liberté et l'autonomie des individus. Mais ils savent aussi piloter nos vies ou *« conduire les conduites »*, selon l'expression de Michel Foucault. Et ils sont désormais dans la boîte à outils de la surveillance de masse.

3) Les biens communs.

C'est un espace de conquête, entre la propriété privée et l'Etat.

Ce rapport marque là aussi une étape. Quand il s'agit de reconnaître un statut en droit positif aux communs et au domaine public, les esprits sont mûrs.

Les communs numériques, les ressources qui permettent à l'internet d'exister sont des biens communs.

C'est aussi dans cette partie que se sont exprimés des désaccords, qui n'ont pas permis d'exprimer des recommandations dans l'esprit d'unanimité qui marque ce rapport.

Je n'en suis pas surpris. Ce n'est pas le temps qui a manqué, que la difficulté à se détacher, sur ce point, du monde ancien.

- **Encore faut-il cerner les désaccords, les explorer et les éclairer. Nous avons tenté de le faire.**

Le débat sur l'évolution de la propriété intellectuelle est inséparable de la révolution numérique. Je suis de ceux qui considèrent que les droits des auteurs, des artistes en général et de ceux qui contribuent à rendre possibles la création et la diffusion des œuvres sont essentiels.

Mais après 15 ans de débat, je sais aussi que ces droits doivent être réécrits ; que les conditions de création, de circulation, de rémunération et les modèles de l'économie de la culture sont profondément bouleversés par le numérique. Que les batailles de retardement privent les Français d'avancées majeures, et de droits nouveaux, et les créateurs de rémunérations nouvelles.

Les nouveaux équilibres à trouver relèvent de ce qu'Edgar Morin nomme *« une politique de civilisation »*.

*

* *

Comment imaginer les suites de ce rapport ?

- D'abord **que les citoyens s'en emparent**, comme d'un manifeste pour un nouvel âge de la démocratie. Le débat sur les libertés numériques est l'un des plus riches de la décennie, comme par ailleurs, la prise de conscience écologie.

- Ensuite **il nourrira le travail du Parlement**, voire celui de l'Union Européenne. Nous le transmettrons au gouvernement, et à Axelle Lemaire. C'est d'ores et déjà une contribution en amont de la loi, avant d'être pour nous une source d'amendements quand ce texte viendra à l'Assemblée nationale.

- Enfin, l'existence pendant un an et demi de cette commission est une invitation à **mieux équiper le Parlement français** pour affronter les conséquences de la révolution numérique.

Demain, d'innombrables questions éthiques, sociales, économiques et culturelles viendront en force. L'explosion des modèles économiques, dont Uber n'est qu'une première illustration, les pressions sur le salariat connecté et le droit du travail, l'urgence d'une fiscalité internationale sur l'économie des données, ou encore la condition juridique de «l'homme augmenté » par les instruments de prothèse : ces exemples montrent l'accélération des défis politiques que nos démocraties doivent affronter sans naïveté, et sans jamais démissionner de notre responsabilité de rendre possible un monde meilleur.

C. INTERVENTION DE MME CHRISTIANE FÉRAL-SCHUHL, AVOCATE SPÉCIALISTE DE L'INFORMATIQUE ET DES NOUVELLES TECHNOLOGIQUES, ANCIENNE BÂTONNIÈRE DE PARIS, CO-PRÉSIDENTE

Monsieur le Président,

Monsieur le co-président,

Chers membres de notre commission,

Mesdames et Messieurs.

Belle initiative – inédite et prospective – que celle de créer cette commission : confronter les réflexions et propositions de parlementaires à celles des acteurs de la société civile, c'est se donner toutes les chances de définir une doctrine et des principes durables en matière de protection des droits et libertés à l'œuvre à l'âge numérique !

Les technologies constituent un terrain d'une extraordinaire richesse. En 30 ans, elles ont bouleversé nos règles sociétales, éducationnelles, institutionnelles, économiques… et bien sûr juridiques.

Dans ce contexte d'évolutions permanentes, la préservation de nos libertés est une préoccupation de première importance qui a conduit notre commission à préconiser 100 recommandations. Vous constaterez que notre Commission s'est concentrée sur les questions de principe qui intéressent les droits et les libertés à l'ère numérique.

Notre démarche initiale a consisté à appréhender l'internet comme un « levier d'accélération démocratique et d'approfondissement des droits et libertés ». Mais, confrontés aux débats politiques et à l'actualité législative, nous avons adopté une démarche résolument défensive en ce qui concerne les libertés.

Deux illustrations :

Le droit au respect de la vie privée. Il s'agit d'un principe fondateur rappelé tant par la Déclaration des droits de l'homme et du citoyen que par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Le droit au respect de la vie privée ne doit pas se heurter au droit à la sécurité. Le citoyen est en droit d'attendre de l'Etat des mesures visant à préserver l'ordre et à assurer la sécurité publique. Il ne s'agit donc en aucun cas d'opposer le droit à la protection à la vie privée au droit à la sécurité. En revanche, il faut donner au citoyen des garanties.

Dans ce contexte, nous préconisons de « repenser la protection de la vie privée et des données à caractère personnel » en responsabilisant chacune des parties prenantes :

- le responsable de traitement doit non seulement se conformer à des obligations légales mais également s'inscrire dans une démarche de responsabilisation (*accountability*), en démontrant à ses clients l'importance qu'il accorde à la préservation de leurs droits afin de mériter leur confiance ;

- l'individu doit, quant à lui, être en mesure de s'autodéterminer dans l'univers numérique, en délivrant un consentement éclairé et effectif au traitement de ses données et en exerçant son libre arbitre et son libre agir.

Dans cet objectif, nous suggérons des mesures pour renforcer l'effectivité des droits au respect de la vie privée et à la protection des données personnelles :

- faire des droits au respect de la vie privée et à la protection des données personnelles des droits fondamentaux constitutionnellement garantis **(Rec. N°47)** ;

- retenir une interprétation large de la notion de donnée à caractère personnelle (y inclure notamment les traces, les identifiants, les pseudos) **(Rec. N°48)** ;

- favoriser la conception et l'utilisation des techniques de *privacy by design* et *privacy by default* **(Rec. 50)** ;

Certaines de nos recommandations visent à donner davantage d'autonomie à l'individu face aux pratiques des sociétés commerciales qui collectent, exploitent et conservent leurs données :

- doter l'individu d'un droit à l'autodétermination informationnelle **(Rec. 58)** ;

- accroître ses droits face aux algorithmes, notamment les algorithmes prédictifs ou à caractère décisionnel : droit d'opposition au profilage, intervention humaine effective, transparence, non-discrimination **(Rec. 66)** ;

- renforcer ses moyens juridiques pour faire cesser un manquement à la législation.

Enfin, il nous apparaît indispensable de mieux encadrer les moyens donnés par le numérique aux services de police et de justice (**Rec. 77)** :

- en soumettant à l'autorisation préalable d'un magistrat judiciaire le recours à certaines techniques d'investigation ;

- ou encore en prévoyant des garanties renforcées pour certaines professions.

<u>La liberté d'expression</u>. Cette liberté fondamentale est protégée par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789.

Nous sommes partis d'un double constat :

- la loi de 1881 sur la liberté de la presse est devenue, avec le numérique, une potentialité ouverte à n'importe qui, n'importe où et n'importe quand. Si elle n'a pas élargi le champ de la liberté d'expression, elle a renforcé l'effectivité de ce droit, c'est-à-dire la capacité des individus à en jouir réellement [(1)] ;

- or, cette avancée a été sévèrement remise en question avec l'adoption de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme et l'annonce de plus amples remises en cause de la loi du 29 juillet 1881. De fait, nous avons assisté depuis deux ans à la remise en cause progressive de cette liberté au prétexte du renforcement de la lutte contre la prolifération des contenus illégaux : blocages administratifs, sortie de certaines infractions de presse de la loi de 1881, création de circonstances aggravantes à raison de l'utilisation d'internet, etc.

Aussi, nous préconisons non seulement de conserver la loi de 1881 sur la liberté de la presse, en la réaménageant, mais également de la renommer « loi sur la liberté d'expression » (**Rec. 14**).

Par ailleurs, nous émettons plusieurs recommandations pour affirmer ou réaffirmer :

- le principe de neutralité technologique, ce qui implique notamment de défendre l'application d'un même taux de TVA, quel que soit le support (**Rec. 16**) ou encore ne pas faire par principe de l'utilisation d'internet une circonstance aggravante (**Rec. 17**) ;

- le recours au juge judiciaire, seul garant constitutionnel des libertés ; il faut limiter les cas de contournement du juge par des autorités administratives (**Rec. 30**) ;

- le régime de responsabilité limitée de l'hébergeur : il ne faut pas créer une troisième catégorie pour les plateformes qui viendrait s'ajouter à celles prévues par la LCEN pour l'hébergeur et l'éditeur (**Rec. 22**).

Je suis consciente que ces travaux ouvrent de nouveaux champs d'exploration, de réflexion et d'interrogations. Je sais qu'il reste d'immenses

---

(1) Conseil Constitutionnel, décision n°2009-580 DC du 10 juin 2009 : internet et aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur liberté d'expression dans ses deux dimensions.

matières à explorer. Je pense néanmoins que ces recommandations permettront d'enrichir les débats à venir.

Au moment de conclure, je voudrais remercier très chaleureusement Monsieur Christian Paul qui m'a fait l'honneur de m'associer à ces travaux. J'ai pu apprécier et mesurer sa force de travail, son dynamisme et sa créativité dans les solutions à proposer.

Je voudrais également remercier tous les membres de la Commission pour leur disponibilité, leur écoute et la qualité de leurs contributions dont j'ai apprécié la richesse et la diversité.

Je voudrais aussi remercier les administrateurs qui ont réalisé un travail rédactionnel considérable, dans des conditions souvent difficiles.

II. DÉCLARATIONS

A. DÉCLARATION DE MMES LES DÉPUTÉES VIRGINIE DUBY-MULLER ET LAURE DE LA RAUDIÈRE, ET DE MM. LES DÉPUTÉS FRANCK RIESTER ET PATRICE VERCHÈRE

Les députés Les Républicains, membres de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, se félicitent de la remise du rapport d'information de la Commission au Président de l'Assemblée nationale

Nous remettons aujourd'hui au Président de l'Assemblée nationale le rapport d'information de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique. Ce rapport, fruit d'un an et demi du travail collectif de députés appartenant à différents partis politiques et de personnalités issues de la société civile, fait des propositions fortes sur les possibilités démocratiques de la révolution numérique.

En particulier, nous proposons de consacrer un droit fondamental à l'information d'intérêt public, en utilisant les possibilités offertes par le numérique pour renforcer l'exigence de transparence démocratique et en améliorant la protection des lanceurs d'alerte.

Nous souhaitons également protéger la liberté d'expression dans l'espace public en affirmant le principe de neutralité technologique et en confortant la place du juge comme son seul garant.

Le respect de la vie privée demeure un droit essentiel à l'ère du numérique : nous mettons en garde contre les tentations de surveillance institutionnelle, et proposons de repenser la protection de la vie privée et des données à caractères personnel.

Enfin, nous estimons nécessaire de définir de nouvelles garanties indispensables à l'exercice des libertés à l'ère numérique, en renforçant le droit d'accès à internet, en consacrant la neutralité des réseaux et en introduisant une régulation spécifique des plateformes.

Nous regrettons cependant l'insertion dans ce rapport d'une cinquième partie sur la propriété intellectuelle, qui n'a pas pu bénéficier du travail collectif effectué pour les autres parties du rapport, malgré l'implication forte de quelques membres. En particulier, aucune audition n'a pu être organisée sur ce sujet, aucune consultation n'a été effectuée, et nous n'avons malheureusement pas pu débattre du fond préalablement à sa rédaction. Il nous semble que la force du rapport réside précisément dans ce consensus que nous avons pu atteindre, quels que soient nos parcours, sur les sujets très divers qui composent les quatre premières parties. Ne faisant pas l'objet d'un accord entre nous, nous craignons que cette cinquième partie amoindrisse la portée globale du rapport et éclipse nos recommandations sur d'autres sujets. Nous étions donc défavorables à sa publication, estimant qu'elle aurait utilement pu faire l'objet d'un travail ultérieur, approfondi, de notre Commission.

B. DÉCLARATION DE MM. PHILIPPE AIGRAIN ET EDWY PLENEL : UNE AVANCÉE IMPORTANTE POUR LE DROIT DE SAVOIR ET UNE OCCASION MANQUÉE POUR LES DROITS CULTURELS

Informaticien pour l'un, journaliste pour l'autre, tous deux acteurs du débat public, nous avons participé assidûment aux travaux de la Commission de réflexion sur le droit et les libertés à l'âge du numérique, depuis sa création en juin 2014. Nous l'avons fait au nom des engagements qui sont les nôtres, au sein de l'association La Quadrature du Net pour Philippe Aigrain, du journal en ligne Mediapart pour Edwy Plenel, deux entités toutes deux créées en 2008 qui ont en commun une défense entêtée des droits individuels des usagers et des libertés collectives des citoyens à l'heure des immenses bouleversements économiques, démocratiques, culturels, géopolitiques, écologiques, etc., qu'accompagne ou provoque la révolution multidimensionnelle dont le numérique est le moteur.

Venus de la société civile, qui plus est de la culture démocratique participative propre à l'univers du Net, nous lui devons un compte-rendu.

1. La question démocratique

Sans autre expérience que celle liée à nos professions et métiers, ce n'est pas sans appréhension ni réserve que nous avons fait le pari de cette réflexion collective, entre députés élus dont la légitimité institutionnelle est un fait acquis et « experts » désignés dont les légitimités peuvent toujours être contestées par d'autres compétences. De ce point de vue, nous devons donner acte à nos deux co-présidents, le député Christian Paul et l'avocate Christiane Féral-Schuhl, d'avoir su créer un climat fructueux d'échange, de participation et de délibération, qui a presque toujours permis de dégager des majorités d'idées, soucieuses d'ouvrir des perspectives partagées dans le souci du bien commun.

Ce fut notamment le cas quand notre Commission fut d'emblée mise à l'épreuve par l'accélération, sous la pression du pouvoir exécutif, d'un agenda parlementaire strictement sécuritaire, à rebours de l'intitulé même de notre instance. Mise en cause de l'État de droit et régression des libertés acquises étaient en effet à l'ordre du jour de la nouvelle – et énième – loi antiterroriste de l'automne 2014 tout comme de la loi relative au renseignement du printemps 2015 – impulsée sous le choc des attentats de janvier. Dans les deux cas, notre Commission a su faire front, en adoptant des recommandations transpartisanes où majorité et opposition parlementaires se sont retrouvées avec des citoyen-ne-s, eux aussi de sensibilités diverses, venus de la société civile sur les mêmes inquiétudes face aux risques d'un pouvoir de police sans contrôle fiable ni limite solide.

Ce consensus, qui ne fut pas très difficile à obtenir, a mis en évidence le fossé grandissant entre une minorité de parlementaires avertis du numérique, familiers de ses usages et curieux de ses inventions, et une majorité de leurs collègues prompts à le diaboliser par peur de la modernité et par méconnaissance de ses réalités. Car c'est peu dire que nous n'avons pas été entendus : les avis de la seule Commission de l'Assemblée nationale où étaient représentées des expertises variées, concrètes et documentées, venues du numérique, de son économie comme de sa démocratie, furent tenus pour quantité négligeable lors des débats dans l'hémicycle. Au lieu de quoi, l'émotion, le fantasme et le simplisme – bref, la politique de la peur – ont tenu lieu de réflexion. À cette occasion, le pouvoir exécutif a confirmé sa tentation absolutiste faute de ce contre-pouvoir vivant et vigilant qu'aurait représenté un parlementarisme libéré de la servitude du présidentialisme.

Si notre Commission a pu si facilement s'accorder, à la fois dans son refus d'évidentes régressions démocratiques et dans sa demande d'un sursaut radicalement

inverse, c'est qu'elle partage cette conviction, affirmée dès les premières lignes de son rapport final, que la révolution numérique appelle l'invention d'une nouvelle culture démocratique, plus approfondie, plus horizontale, plus partagée. Bien au-delà des étiquettes partisanes, tant la ligne de clivage traverse toutes les familles politiques, les débats autour des enjeux inédits soulevés par les bouleversements en cours de façon de plus en plus accélérée mettent en évidence la faiblesse de notre écosystème démocratique, ses retards et ses fragilités. Tandis que nos travaux s'efforçaient d'affronter patiemment ce défi, qui est au ressort de notre sourde crise politique, de ses silences comme de ses impatiences, les coups de force sécuritaires imposés en urgence par le gouvernement, sans expertise fouillée ni bilan véritable des dispositions déjà en vigueur – et de leurs échecs manifestes –, témoignaient de ce que notre pays est encore, hélas, une démocratie de basse intensité, superficielle, verticale et confisquée, tant elle dépend de la volonté d'un seul, en lieu et place de la mobilisation de tous.

2. Le droit de savoir

« *La démocratie*, soulignait à l'inverse Pierre Mendès France dans *La vérité guidait leurs pas* (1976), *c'est beaucoup plus que la pratique des élections et le gouvernement de la majorité : c'est un type de mœurs, de vertu, de scrupule, de sens civique, de respect de l'adversaire ; c'est un code moral*. » Il reviendra, espérons-le, à d'autres assemblées de fonder, institutionnellement, cette culture démocratique nouvelle qui nous libérera de la fascination pour le pouvoir personnel où s'épuise, voire se nécrose, notre vie publique. Mais, sans attendre cette échéance, la démocratie est déjà notre affaire, ici et maintenant. Le principal acquis des travaux de notre Commission et de son rapport final est de l'affirmer fortement et concrètement sur le terrain de deux libertés fondamentales, sans l'épanouissement desquels l'exercice du droit de vote peut n'être qu'une comédie des apparences, une liberté minée de l'intérieur parce que corrompue par les propagandes et les mensonges, les illusions idéologiques ou communicantes : le droit de savoir et la liberté de dire.

En plaçant la question du droit de savoir – droit de connaître tout ce qui est d'intérêt public, droit d'accès, droit de communication, droit de diffusion, etc. – avant celle de la liberté de dire – liberté d'expression, d'opinion, de conviction, de point de vue, etc. –, notre rapport met l'accent sur une question politique centrale que posait Hannah Arendt dans un texte célèbre de 1967, *Vérité et politique* : « *La liberté d'opinion est une farce si l'information sur les faits n'est pas garantie et si ce ne sont pas les faits eux-mêmes qui font l'objet du débat* ». Posant que les « *vérités de fait* », qu'il s'agisse du présent ou du passé, sont « *les vérités politiquement les plus importantes* », la philosophe mettait au centre de la vie démocratique la question du libre accès des citoyens aux informations d'intérêt public qui, les concernant au premier chef, ne sauraient être confisquées par les pouvoirs, étatiques ou économiques, nationaux ou transnationaux, tenues au secret ou couvertes par l'opacité. S'appuyant sur les potentialités nouvelles – d'accès facile, d'archivage infini et de partage démultiplié – ouvertes par les technologies numériques, notre rapport met en évidence l'immense retard démocratique de la France en ce domaine du droit à l'information.

Tel est pour nous l'acquis principal de ce rapport dont nous appelons tous les citoyen-ne-s à se saisir : exiger la consécration d'un droit fondamental à l'information d'intérêt public, non seulement par la loi mais par diverses dispositions qui sont détaillées dans les propositions énoncées. Loin d'en faire un enjeu limité aux métiers de l'information, elles placent cette question du droit de savoir au ressort de la vie démocratique, comme un enjeu citoyen que le surgissement des lanceurs d'alerte concrétise. C'est donc à la société de s'emparer de ce qui est ici affirmé et revendiqué, tant il est à craindre que ce rapport, hélas, reste lettre morte. De fait, malgré ses engagements électoraux de 2012, l'actuelle majorité parlementaire, réduite à sa discipline présidentielle, a pour l'heure remisé sa promesse d'une

nouvelle loi protégeant réellement le secret des sources, alors même qu'elle adoptait une loi sur le renseignement qui, potentiellement, le met en péril.

Les quatre premières parties de ce rapport ont donc notre entière approbation, avec le souhait qu'elles servent de base, demain ou après-demain, à ce sursaut démocratique dont notre pays a urgemment besoin, en redonnant au peuple lui-même la capacité d'inventer et de délibérer de façon informée, par l'accès le plus large aux savoirs et aux connaissances. En revanche, tout en approuvant avec ses limites le compromis final énoncé dans la cinquième partie, nous regrettons que, faute de temps et de débats, notre Commission ait échoué à produire une avancée de la même ampleur sur la question des droits culturels.

3. Les droits culturels

Le contexte

L'irruption du numérique, a représenté un véritable séisme pour la réflexion sur les droits à l'égard des œuvres, notamment à partir des années 1990, lorsque l'usage massif du Web s'est ajouté à celui l'informatique. Vingt ans plus tard, un fossé considérable s'est creusé entre le droit et les pratiques culturelles, mais aussi entre les différents acteurs de ce qui est devenu un écosystème complexe, où s'affrontent et s'allient aujourd'hui au moins quatre catégories d'acteurs : le public, les contributeurs à la création (auteurs, interprètes, techniciens), les éditeurs et producteurs et enfin les distributeurs et fabricants de matériels et logiciels pour ces matériels. Par ailleurs, des acteurs institutionnels comme les sociétés de perception et de répartition de droits, qui jouent ou pourraient jouer un rôle important de gestion collective pour tous les créateurs sont souvent contrôlés par les éditeurs, les héritiers et les gros bénéficiaires et interviennent de façon dominante dans le lobbying concernant l'évolution du droit d'auteur

Nous voulons ici affirmer avec force qu'il est possible de servir ensemble les droits des auteurs et autres contributeurs à la création, le financement des activités créatives, le partage et la diversité de la culture. Mais que ce n'est possible qu'à condition de dépasser certaines incompréhensions concernant ce qui est en jeu dans l'espace numérique et de rompre avec certains dogmes.

Face à l'irruption du numérique, la réaction des acteurs en place a été marquée par un contresens majeur mais compréhensible. Ils ont été obnubilés par la perte de leur contrôle sur la circulation des œuvres, et sidérés que cette perte s'effectue au profit de ceux-là même qui sont leurs clients : les individus qui apprécient les œuvres.

Les industries culturelles lancèrent ainsi une campagne pour empêcher les individus de partager les œuvres entre eux et pour pouvoir contrôler dans le détail leurs usages de celles-ci aux moyens de dispositifs techniques. Elles appelèrent « respect des droits d'auteur (ou du copyright) » et adaptation de ceux-ci à l'ère numérique cette offensive pour empêcher le développement de pratiques constitutives du Web (la copie, le partage, la réutilisation) lorsqu'elles portaient sur des œuvres soumises au droit d'auteur, même lorsque ces pratiques se développaient sans but de profit.

Cette approche reposait sur diverses erreurs ou omissions :

- L'ignorance encore très commune aujourd'hui que le numérique est avant tout un espace de création et de participation, que la culture se produit sur le Web, s'y diffuse nativement.

- Point lié essentiel : l'immense augmentation du nombre des personnes impliqués dans les activités créatives et des œuvres qu'elles produisent, et son corollaire mécanique, la baisse de l'audience moyenne de chacun. Il s'agit là du défi principal

de l'ère numérique, auquel on peut réagir soit en concentrant l'attention sur un nombre réduit d'œuvres, soit en explorant de nouveaux modèles de financement non dépendants de la seule audience.

- La négligence du fait que les biens culturels avaient toujours fait l'objet d'un partage assez large, même si significativement moindre que celui rendu possible par le numérique. Ainsi plus d'une lecture sur deux d'un livre physique ne donnait lieu, dès avant le numérique, à aucune transaction monétaire ni à revenus pour l'auteur ou l'éditeur.

- Enfin le fait qu'en Europe, jusqu'à très récemment, les actes non marchands de toutes sortes, même lorsqu'ils sont soumis aux droits exclusifs du droit d'auteur donnaient très souvent lieu à des relaxes, et ne donnaient à peu près jamais lieu à des sanctions dépassant quelques centaines d'€[1].

Le bilan de l'approche qui fut activement poursuivie par les pouvoirs exécutifs et acceptée par les législateurs est fort peu satisfaisant :

- En traitant les citoyens en ennemis et en manifestant une incompréhension de leurs pratiques numériques, puis en menant une guerre spécifiquement ciblée contre les réseaux pair à pair, les éditeurs et producteurs les ont poussés dans les bras des distributeurs et fournisseurs de technologies et des systèmes de streaming ou téléchargement centralisés.

- Alors que toutes les études sur les souhaits des usagers montrent que les citoyens souhaitent rémunérer les créateurs et les activités éditoriales, ce qui est confirmé par le développement fort du financement participatif et le succès des logiques d'abonnement et de soutien, alors que les individus consacrent des sommes significatives à l'achat des matériels et services leur permettant de produire et échanger des œuvres, on a retardé considérablement l'évolution des industries culturelles vers des activités qui mobilisent cet engagement.

- Le chiffre d'affaires global des différents médias (musique comprise) a continué à progresser mais dans un contexte d'inégalités croissantes entre œuvres, entre créateurs, entre ceux-ci et les détenteurs de rentes de droits. En d'autres termes avec une diversité culturelle réduite[2].

- Les contrefaçons commerciales n'ont pas décru et les nouvelles mesures envisagées pour y mettre fin font craindre de sévères débordements portant atteinte aux droits fondamentaux : ainsi par exemple de la privation de ressources pour des sites ou acteurs désignés par des acteurs privés qui étend à ce domaine les méthodes utilisées par le gouvernement américain pour tenter d'étouffer Wikileaks.

Puisque le passé est déjà écrit, peut-on faire mieux dans le futur ? Nous en sommes convaincus, et nous sommes convaincus que c'est à cette condition qu'une vraie adaptation du droit d'auteur au numérique sera possible.

---

1 *Source : Bernt Hugenholtz, exposé au séminaire du réseau européen COMMUNIA, Amsterdam, 20 October 2008. Cette situation est très différénte de celle des États-Unis ou des condamnations à plusieurs centaines de milliers d'euros ont eu lieu.*

2 *Sur ce point voir Ph. Aigrain, Sharing : Culture and the Economy in the Internet Age, Amsterdam University Press, 2012.*

Comprendre l'écosystème et y favoriser de nouvelles synergies

Revenons aux quatre catégories d'acteurs listées plus haut, et prenons acte des profondes transformations que le numérique y a provoquées.

- Le public ne peut plus être compris comme constitué de consommateurs ou d'usagers : une part très importante des personnes de plus de 16 ans (au moins le quart dans les pays européens).
- La distinction entre créateurs professionnels et amateurs a été remplacée par un continuum de positions où la très grande masse des créateurs sont dans des statuts mixtes et souvent précaires, mêlant différentes sources de revenus, dont beaucoup ne sont pas directement liés à leurs pratiques et d'autres prennent la forme d'honoraires, de cachets, de prestations salariées ou de soutiens directs de la part du public.
- L'édition et la production sont des mondes fragmentés, où les petits éditeurs, labels et producteurs indépendants jouent un rôle clé dans l'incubation et l'accompagnement de la création alors que les grandes sociétés qui capturent une grande part des marchés se concentrent sur la promotion d'un petit nombre de titres dans des cycles de plus en plus courts.
- Enfin, les distributeurs, producteurs de matériels mobiles et logiciels pour ces matériels sont de plus en plus intégrés verticalement, capturent une part accrue de la valeur et structurent les marchés et l'évolution des technologies selon leurs intérêts. Les majors prennent parfois le contrôle partiel ou total de distributeurs secondaires (Spotify, Deezer) mais sans jamais concurrencer les acteurs dominants (Google/Youtube, Apple, Amazon).

Comment sortir de ce cycle infernal où les seuls bénéficiaires sont les acteurs oligopolistiques, principalement les plateformes, secondairement les majors de l'édition ? C'est évidemment en reconnaissant enfin des droits au public et en construisant et soutenant des synergies positives entre lui, les auteurs et interprètes et les acteurs éditoriaux et de médiation innovants.

Repartir du socle des droits fondamentaux

Tout au court du travail de la commission, nous nous sommes basés sur les droits culturels fondamentaux. Définis dans la Déclaration universelle des droits de l'Homme (article 27) et dans le Pacte des droits sociaux économiques et culturels (article 15 notamment), ils affirment en parallèle les droits de chacun à participer à la vie culturelle de la cité et ceux des auteurs (au sens large) à voir leurs intérêts moraux et matériels protégés. Sur ce dernier point, la déclaration comme le pacte sont agnostiques en ce qui concerne les moyens à employer, droits exclusifs ou toute autre méthode.

Les droits fondamentaux doivent à chaque époque être interprétés en prenant en compte les conditions concrètes de leur exercice. C'est d'ailleurs ce qu'a fait le Conseil Constitutionnel lorsque dans sa décision du 10 juin 2009 il a affirmé l'accès à internet comme condition de l'exercice du plus important de tous les droits du point de vue de la démocratie, la liberté de pensée et d'expression. La prise en compte des droits culturels appelle le même effort d'actualisation. Conscients que cette prise en compte qui suppose une réorientation du cours dominant de l'évolution des droits ne serait que progressive, nous avons mis sur la table une pragmatique et modérée, minimale, même. Tout en invitant le législateur à animer les débats futurs sur une définition plus large des droits culturels des individus dans la sphère non marchande, nous lui avons recommandé de faire de petits pas dans la direction des droits minimaux des usagers et des auteurs, selon quatre aspects.

- Le premier consiste à qualifier certaines des exceptions et limitations existantes dans notre droit de droits culturels d'usage et de renforcer la capacité pratique à les exercer en affirmant que lorsque des mesures techniques de protection (MTP, aussi connues sous le nom de DRM) font obstacle à l'exercice des exceptions, les MTP ne peuvent être protégées pour le contournement lorsque ce contournement est effectué pour les besoins de cet exercice. Cette approche est parfaitement compatible avec le droit européen et a été appliquée par de nombreux pays lors de la transposition de la directive 2001/29/CE (DADVSI).

- Le second consiste à élargir le champ de certains de ces droits culturels d'usage (des exceptions et limitations correspondantes) qui sont déjà présents dans notre droit national. Il s'agit par exemple d'affirmer dans la loi que le droit de citation s'applique à tous les médias dans des conditions appropriées à chacun ou que les exceptions de parodie et satire ne sont pas restreintes à l'usage comique.

- Le troisième enfin consistait à faire une premier pas vers la reconnaissance des pratiques de la culture numérique en soutenant au niveau européen la création d'une exception pour les pratiques de remix et de mashup.

- Enfin, dans le champ des droits des auteurs, nous souhaitions qu'en particulier dans le champ du texte si essentiel au futur de notre démocratie[1], une nouvelle loi sur le contrat d'édition revoit celle adoptée par ordonnances à la suite de négociations très difficiles et très inégales entre éditeurs et auteurs. La recommandation 98 a repris en l'élargissant à d'autres médias cette approche et nous nous en félicitons, tout en regrettant qu'elle reste imprécise dans son rapport au droit actuel et à son application[2].

Quand même les droits les plus minimaux sont rejetés

Notre approche était si pragmatique que nous avons proposé nous-mêmes de renoncer au troisième volet que nous jugeons pourtant essentiel pour une véritable « mutation numérique » du droit d'auteur. Malgré cela, nous nous sommes heurtés en ce qui concerne les droits d'usage minimaux à une opposition de principe d'un petit nombre de membres de la Commission opposant la lettre du droit existant à ce que nous affirmons être les conditions réelles de son application.

Pourquoi un tel blocage ?

Le droit d'auteur n'était certainement pas le seul sujet traité par notre commission pour lequel existaient des divergences de vue entre ses membres. Cependant, d'autres cas, la mission d'expliciter de nouveaux droits pour l'âge numérique a prévalu, et nous devons remercier les membres de la commission qui ont ainsi permis que des recommandations fortes et claires soient formulées.

Quelle est donc la spécificité du droit d'auteur de ce point de vue ? Quels facteurs ont joué pour aboutir à une telle crispation en faveur du statut quo ? Il est probable que la prévalence d'une approche juridique centrée le droit matériel existant et non sur son devenir souhaitable a joué. Mais une autre source de blocage provient de ce que l'objet réel des débats sur le droit d'auteur est en réalité plus large que son appellation le laisse supposer.

---

1 Ce n'est évidemment pas le seul et c'est une des raisons pour lesquelles l'application d'un vrai droit de citation à l'audiovisuel est essentielle.

2 Par exemple : le droit actuel établit que seuls les auteurs peuvent autoriser l'application de DRM à leurs œuvres mais en pratique leur capacité à refuser de le faire est très faible voir nulle ; l'existence de contrats séparés à durée limitée pour le numérique est essentielle dans plusieurs médias et ne saurait être remplacée par une clause de révision dont l'exercice pratique se heurtera à des conditions d'inégalité similaires à celles de la signature du contrat initial.

Dans de très nombreux cas, il ne s’agit pas des droits des auteurs mais aussi des intérêts des éditeurs, producteurs, distributeurs ou fournisseurs de technologies et services ou plus récemment des droits (ou de leur absence) pour le public. Nous espérons que notre contribution aura contribué à rendre visible cet élargissement du champ, à y cerner synergies et contradictions et qu’elle contribuera au développement d’une culture des droits culturels fondamentaux en France et en Europe.

III. CONTRIBUTIONS AU GROUPE DE TRAVAIL SUR LA VIE PRIVÉE

A. CONTRIBUTION DE M. WINSTON MAXWELL : LA NOTION DE CONSENTEMENT

Le consentement est l'un des fondements de la protection des données à caractère personnel. Reconnue comme un droit fondamental en Europe, la protection des données personnelles est un élément de la liberté individuelle : sans une certaine maîtrise de ce qui est divulgué à propos de soi, l'individu perd son autonomie par rapport aux autres. Le contrôle par chaque individu de ses données va donc au cœur de l'autodétermination informationnelle de l'individu [(1)].

Traditionnellement, cette maîtrise sur les données à caractère personnel se manifeste à travers le consentement de l'individu. Si l'individu donne son consentement, il exprime sa liberté de choix par rapport à ses données à caractère personnel. Un consentement éclairé et librement consenti permet de procéder à la plupart des traitements de données à caractère personnel. L'autonomie de chacun est respectée.

Dans un environnement numérique, le consentement trouve néanmoins ses limites. Comme l'a exprimé la Présidente de la CNIL devant notre Commission, chaque individu est entouré d'une multitude de traitements par de nombreux réseaux et services numériques qui régissent une partie de nos vies en permanence. Dans ce contexte, l'idée que chaque individu peut donner son consentement pour chaque traitement est illusoire.

Selon le Conseil d'État :

« Le rôle du consentement de la personne ne doit être ni surestimé (dans la législation actuelle, il n'est ni une condition nécessaire ni une condition suffisante de la licéité du traitement des données), ni méconnu, car il incarne la liberté de la personne en matière d'utilisation de ses données personnelles » [(2)].

La plupart des fournisseurs de services numériques s'appuient sur des conditions générales d'utilisation. Avant d'utiliser le service, le consommateur coche une case indiquant qu'il a lu les conditions et qu'il les accepte. Comme l'a souligné le Conseil d'État dans son étude de juillet 2014 [(3)], même le consommateur le plus attentif ne pourra prendre le temps de lire ces conditions d'utilisation. Et même s'il prenait le temps, le consommateur ne serait pas en mesure d'apprécier les risques encourus par telle ou telle utilisation de ses données personnelles. Les risques sont abstraits, et les conditions d'utilisation ne permettent pas de les apprécier. Par ailleurs, les fournisseurs de service ne sont pas en mesure d'offrir une alternative au consommateur. Si le consommateur souhaite utiliser un service numérique, il doit accepter les conditions d'utilisation telles qu'elles. Un grand nombre de ces services sont fournis gratuitement, ce qui signifie que leur modèle économique peut s'appuyer sur la vente de publicités. La vente de publicités s'appuie à son tour sur l'analyse de données à caractère personnel. Si le consommateur souhaite bénéficier d'un service gratuit, il devra généralement accepter que le service utilise ses données.

Les conditions d'utilisation étant trop longues, le consentement de l'individu peut également être sollicité par des fenêtres *pop-up* que le consommateur accepte au fur et à

---

(1) Conseil d'État, op. cit.*, p. 268.*

(2) Ibid*, p. 18.*

(3) Ibid.*, p. 176.*

mesure de son utilisation du service. L'utilisation répétée de fenêtres *pop-up* peut agacer le consommateur au point où il ne regarde plus les messages et les accepte systématiquement.

Le consentement s'avère donc souvent inefficace. Ce constat est appuyé par de nombreuses études en psychologie et en économie comportementale. Acquisti *et al.* [(1)] ont démontré que la plupart des individus attachent une valeur faible à la protection de leurs données personnelles. Dans leur étude, 71 % des personnes ont accepté d'échanger leur mot de passe contre une barre de chocolat. Dans une autre étude, l'équipe d'Acquisti a démontré que les consommateurs qui bénéficient de mécanismes de contrôle de leurs données sur une plateforme numérique sont plus susceptibles de communiquer des données sensibles. Donner plus de moyens de contrôle aux consommateurs peut paradoxalement les inciter à être moins vigilantes [(2)].

D'autres tests confirment que les consommateurs ne lisent pas ce qu'ils acceptent : dans une expérimentation, 7 500 personnes ont donné leur accord pour céder leur âme pour l'éternité à un fournisseur de service :

« Hardly anyone reads privacy policies. To give an example, an English company obtained the soul of 7500 people. According to its terms and conditions, customers granted "a non transferable option to claim, for now and for ever more, your immortal soul," unless they opted out. The company later said it wouldn't exercise its rights » [(3)].

Ces phénomènes commencent à être bien compris par les psychologues et les économistes.

Si le consentement est une fausse bonne idée, que proposer à sa place ?

Dans la législation actuelle, le consentement n'est pas le seul fondement pour un traitement. Il existe notamment la notion « d'intérêt légitime » accompagné de mesures destinées à protéger les individus. L'intérêt public peut également justifier, dans certains cas, un traitement sans le consentement de l'individu [(4)].

Nissenbaum [(5)] propose d'imposer des règles de traitement qui varieraient selon le contexte dans lequel les données sont collectées. Cette approche reconnaîtrait un consentement implicite pour tout traitement qui découlerait naturellement du contexte d'origine de la collecte de données. Un traitement qui sortirait de ce contexte nécessiterait un consentement explicite. Cette idée n'est pas loin de celle du groupe article 29 (G29), qui reconnaît la possibilité d'effectuer des traitements pour des finalités qui ne sont pas "incompatibles" avec la finalité d'origine [(6)]. Une finalité « incompatible » nécessiterait le recours à un consentement explicite. Une finalité « compatible » ne nécessiterait pas de consentement.

Le Forum économique mondial préconise la notion d'« empowerment » au lieu de la notion plus formaliste de consentement [(7)].

---

(1) A. Acquisiti, L. John, G. Loewenstein, « What is privacy worth ? », 2004.

(2) L. Brandimarte, A. Acquisit, G. Loewenstein, « Misplaced confidences : privacy and the control paradox », WEIS Working Paper*, 2010.*

(3) F. Z. Borgesius, « Consent to behavioural targeting in european law – What are the policy implications of insights from behavioural economics ? », Amsterdam Law School Legal Studies Research Paper*, n° 2013-43, p. 31.*

(4) Article 7 de la loi n° 17-78 du 6 janvier 1978 précitée.

(5) H. Nissenbaum, « Privacy as Contextual Integrity », Wash. L. Rev.*, 2004.*

(6) Article 29 Working Party, « Opinion 03/2013 on Purpose Limitation », WP 203*, 2 april 2013.*

(7) World Economic Forum, « Unlocking the value of personal data : from collection to usage », février 2013. Voir également Conseil d'État, op. cit.*, p. 170.*

Constatant l'inefficacité du consentement dans un environnement numérique, Borgesius [1] propose que le législateur définisse une zone d'utilisations « normales » de données, par exemple en matière de publicité ciblée. À l'intérieur de cette zone de normalité, le consentement du consommateur ne serait pas nécessaire. En revanche, une utilisation qui sortirait de cette zone de normalité nécessiterait un consentement renforcé. Ce consentement renforcé se manifesterait par au moins 3 clics de souris, par exemple, ou par un appel téléphonique, ou par l'envoi d'une lettre... Pour certains types de traitement, le législateur pourrait imposer une interdiction totale. C'est le cas en France, par exemple, pour les traitements de données ADN en dehors de la recherche médicale.

La difficulté pour le législateur serait de définir ces « zones de normalité », qui peuvent évoluer avec le temps. La définition nécessiterait une étude d'impact, et la prise en compte d'aspects dynamiques, autant culturels et économiques. Ce travail pourrait être confié au régulateur, par exemple à la CNIL en France.

La CNIL effectue déjà ce genre d'évaluation lorsqu'elle élabore des normes simplifiées ou des autorisations uniques pour certains traitements. Ces normes simplifiées et autorisations uniques définissent une zone de traitement acceptable à l'intérieur de laquelle le consentement individuel n'est généralement pas nécessaire. Cette piste pourrait être privilégiée, le consentement étant réservé à des utilisations qui sortent de l'ordinaire et qui surprennent par rapport au contexte d'origine de la collecte [2].

---

(1) F. Z. Borgesius, « Consent to behavioural targeting in european law – What are the policy implications of insights from behavioural economics? », Amsterdam Law School Legal Studies Research Paper, *n° 2013-43.*

(2) Selon le Conseil d'État, « collecter des données de manière déloyale, c'est surprendre la confiance de la personne concernée et commettre ainsi une faute à son égard » in *Conseil d'État*, op. cit., *p. 173.*

B. CONTRIBUTION DE M. DANIEL LE MÉTAYER : ANALYSER ET PRÉVENIR LES RISQUES D'ATTEINTE À LA VIE PRIVÉE

Au-delà de la protection des données personnelles

La notion de vie privée est difficile à définir précisément et sujette à évolutions et à interprétations variées selon les époques et les cultures. Le développement massif des technologies numériques a encore compliqué la donne en introduisant de nouvelles pratiques de dévoilement de soi et en permettant la collecte massive de données personnelles. Les lois régissant la collecte et l'usage des données personnelles constituent des instruments majeurs de protection de la vie privée à l'ère numérique. Cependant, leur application se heurte à de nombreuses difficultés : par exemple, les contrôles *ex ante* (déclarations, demandes d'autorisation, etc.) sont de plus en plus inadaptés dans une société de circulation permanente de données ; la notion même de donnée personnelle, qui est au cœur du dispositif, est sujette à débats (trop large pour certains, insuffisante pour d'autres), de même que celle de responsable de traitement ou de finalité (à l'heure du *big data*, qui inverse la logique, les données précédant la finalité). Le règlement européen sur la protection des données personnelles en cours de discussion [(1)] tente d'apporter des réponses à ces questions, notamment en mettant l'accent sur les contrôles *ex post* (en particulier en renforçant la responsabilité (ou *accountability*), les analyses d'impact (*data protection impact assessment*), et la protection de la vie privée par construction (*privacy by design*). Cependant, même si ce règlement (dans sa version actuelle) comporte un certain nombre d'avancées, il n'aborde pas de façon frontale des questions centrales comme celles des frontières entre données personnelles et données anonymisées, ou entre données sensibles et données non sensibles.

Données anonymisées, données personnelles, données sensibles : un continuum plutôt que des catégories distinctes.

Les questions actuelles sur l'anonymisation illustrent parfaitement les limites des visions dualistes en matière de données personnelles. Les enjeux en la matière sont majeurs, aussi bien pour le développement durable d'une industrie de l'analyse de données que pour la réalisation de programmes de recherche d'intérêt public, dans le domaine de la santé notamment. D'un point de vue juridique, des données anonymisées sortent du périmètre de la loi Informatique et Libertés [(2)]. Statuer sur le caractère anonyme ou pas d'une donnée n'est donc pas une décision anodine. Or les spécialistes du sujet s'accordent pour dire qu'on ne peut jamais assurer qu'un jeu de donnée est absolument anonyme dès lors qu'il est issu de données personnelles [(3)]. Bien entendu, l'anonymisation peut être utilisée dans des contextes très variés depuis la production de données démographiques à l'échelle d'un pays (dont personne n'envisagerait de contester la publication) à la génération de jeux de données prétendument anonymisés qui ont été facilement exploités pour réidentifier les personnes concernées (affaire Netflix, dévoilement des données de santé du gouverneur du Massachussetts, publication des trajets de taxis de New York City dans le cadre de la

---

(1) Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation), *texte adopté par le Parlement européen le 12 mars 2014.*

(2) Comme de la directive n° 95-46 CE et du projet de règlement européen sur la protection des données personnelles dans sa version actuelle. Cependant, les dispositions juridiques intéressant la protection de la vie privée restent, le cas échéant, applicables.

(3) P. Ohm, « Broken promises of privacy : responding to the surprising failure of anonymization », University of Colorado Law Legal Studies Research Paper, *n° 09-12.*

Freedom Of Information Law, etc.). Ces exemples de réidentification [1] ne sont guère surprenants puisqu'il a été montré que 4 positions géographiques suffisent à identifier de manière unique 95 % des personnes [2] ou encore que 87 % des citoyens américains pouvaient être identifiés de manière unique à partir de seulement 3 informations [3] (date de naissance, code postal et genre).

Si la frontière entre données personnelles et données anonymes n'est pas facile à définir, on peut en dire tout autant de celle qui sépare données sensibles et données non sensibles. Les premières, pour lesquelles un consentement exprès est exigé, sont définies de manière énumérative (dans la loi Informatique et Libertés comme dans la directive n° 95-46 CE) et comprennent « les données qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » [4]. Cependant, l'analyse de certaines données de géolocalisation permet de déduire toutes sortes d'informations sensibles. De fait, toute liste fermée pourra être sujette à discussion. Ces doutes ont amené certains à proposer une redéfinition des données sensibles reposant sur une analyse des risques de préjudices aux individus [5]. Une telle démarche permettrait de dépasser la vision binaire qui domine actuellement pour envisager plutôt les données dans un continuum, allant des données les plus anodines aux données personnelles les plus sensibles.

Une démarche d'analyse de risques.

Les exemples précédents illustrent le fait qu'il faut se garder d'une vision trop « fétichiste » de la donnée personnelle. Nombre de juristes et de philosophes ont proposé de concevoir la protection des données personnelles comme un moyen, un instrument au service de la protection de la vie privée, plutôt qu'une fin en soi. Mais comment assurer l'effectivité d'un droit comme celui de la vie privée qu'on ne parvient pas à caractériser précisément ?

On peut observer que s'il n'est effectivement pas aisé de cerner précisément les contours de ce droit, ses violations, même si elles sont de natures très variées, sont généralement perçues sans difficulté. Une option consiste donc à envisager les mesures de protection de la vie privée à travers le prisme des préjudices qui peuvent être causés par ces violations. Le cœur de cette démarche doit être une analyse précise des risques posés par les collectes et les traitements de données, une mise en regard de ces risques avec les intérêts des traitements (pour le sujet mais aussi pour la société de manière plus générale) et, si le traitement est mis en œuvre, l'étude des techniques les plus à même de minimiser ces risques. Cette démarche, si elle s'accompagne des garanties suffisantes [6], peut conduire à des protections à la fois plus réalistes (effectives) pour les sujets tout en favorisant le

---

(1) Terme impropre, strictement parlant, puisque ces jeux de données étaient en fait mal anonymisés (en réalité pseudonymisés) mais ces confusions illustrent la nécessité d'une démarche plus rigoureuse en la matière.

(2) Étude réalisée à partir d'un jeu de données représentant les positions géographiques horaires définies au degré de précision des périmètres des antennes de téléphones mobiles : Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, V. D. Blondel, « Unique in the crowd : the privacy bounds of human mobility », Scientific Reports, Nature , *mars 2013.*

(3) L. Sweeney, « Simple demographics often identify people uniquely », Carnegie Mellon University, Data Privacy Working Paper 3, *Pittsburgh 2000.*

(4) Article 8 de la loi n° 78-17 du 6 janvier 1978 précitée.

(5) P. Ohm, « Sensitive information », 2014, Southern California Law Review, *vol. 88, 2015, Forthcoming,* http://papers.ssrn.com/sol3/papers.cfm?abstractid=2501002.

(6) Working Party 29, Statement on the role of a risk-based approach in data protection legal frameworks, *texte adopté par le Groupe de l'article 29 le 30 mai 2014.*

développement de l'analyse de données à grande échelle, aussi bien à des fins économiques que pour le bien public.

Cependant plusieurs conditions doivent être réalisées pour atteindre ces objectifs. Il faut notamment pouvoir :

- répertorier et caractériser les préjudices potentiels résultant des atteintes à la vie privée ;
- définir des méthodes d'analyse de risques rigoureuses et documentées de sorte que toutes les décisions prises puissent être tracées et justifiées (selon le principe de redevabilité ou *accountability*) ;
- en fonction des risques identifiés, choisir et dimensionner les mesures (techniques, organisationnelles, juridiques) à prendre par les responsables de traitement.

De plus, cette démarche ne doit pas conduire à limiter les droits des individus [(1)], notamment en matière de données personnelles (droits d'accès, de rectification, d'effacement, *etc*) ou à remettre en cause des principes fondamentaux (légitimité, minimisation des données, finalité, *etc*).

Les préjudices résultant des atteintes à la vie privée

Si la notion de protection de la vie privée résiste à toute tentative de définition précise, les atteintes à la vie privée sont généralement plus faciles à cerner [(2)]. Plusieurs classifications de ces préjudices ont d'ailleurs été proposées. Par exemple, Ryan Calo [(3)] a distingué les préjudices « subjectifs » qui sont provoqués par le seul fait de se savoir (ou de se croire) observé, des préjudices « objectifs » découlant d'une utilisation inattendue ou imposée de données aux détriments de la personne concernée. Pour sa part, Paul Ohm [(4)] a distingué trois grandes catégories de préjudices, selon un critère historique :

– les préjudices « de première génération » qui se mesurent les plus facilement (parfois même de manière financière) dans lesquels il inclut les violations de confidentialité, la diffamation, le chantage, le vol d'identité et le harcèlement ;

– les préjudices « traditionnels » définis au début du 20e siècle par les juges Warren et Brandeis qui ont œuvré pour la reconnaissance de « blessures aux sentiments » [(5)]. Cette catégorie inclut notamment les atteintes à la dignité et à la personnalité, l'humiliation, la honte. Elle concerne par exemple la révélation publique d'événements liés à la santé, aux pratiques sexuelles, ainsi que toute information qui pourrait paraître humiliante ou ostracisante pour la personne concernée ;

– les préjudices « modernes » sont liés à la perte de contrôle sur ses informations personnelles et concernent non seulement les personnes mais aussi les groupes et la société de manière plus générale. Ce qui est en jeu pour les individus, c'est la perte d'autonomie et de capacité à développer sa personnalité. On peut ranger dans cette catégorie les

---

(1) Working Party 29, Statement on the role of a risk-based approach in data protection legal frameworks, *texte adopté par le Groupe de l'article 29 le 30 mai 2014.*

(2) Même si des positions divergentes peuvent apparaître dans certains cas limites, notamment quand la protection de la vie privée entre en conflit avec d'autres impératifs comme la liberté d'expression, le droit d'information ou la sécurité des personnes. Mais ces divergences portent plus sur le poids relatif des différents droits que sur la réalité d'un préjudice.

(3) R. Calo, The boundaries of privacy harm, Indiana Law Journal, *Vol. 86, No. 3, 2011.*

(4) D. Solove, A taxonomy of privacy, Universitry of Pennsylvania Law Review, *Vol. 154, No. 3, 2006.*

(5) « mere injury to the feelings *» : S. D. Warren, L. D. Brandeis, « The right to privacy »,* Harvard Law Review, *193 (1890).*

discriminations, les manipulations, l'uniformisation des comportements (conformisme anticipatif) lié au sentiment de surveillance ainsi que les conséquences sur la vie démocratique elle-même (moindre volonté de s'exprimer, appauvrissement du débat public).

La proposition la plus complète en la matière reste cependant celle du juriste américain Daniel Solove qui a défini une taxonomie organisée selon les principaux types d'activités qui peuvent donner lieu à des préjudices (pour les individus ou pour la société) : la collecte d'information, leur traitement, leur dissémination et l'« invasion » (intrusion notamment) :

– les préjudices liés aux collectes d'information englobent notamment toutes les conséquences de la surveillance (inconfort, auto-censure, inhibition, conformisme, atteinte à la dignité, etc.).

– les préjudices liés aux traitements d'information comprennent les incidences de l'agrégation et de l'analyse de données qui induisent un déséquilibre informationnel entre les individus et les entités privées ou publiques [(1)], avec finalement des effets semblables à ceux de la surveillance. Ils incluent également les conséquences de l'identification (atteinte à la liberté de circuler ou de s'exprimer de façon anonyme, sentiment de traçage, réduction ou assignation à une identité, etc.) et des vols d'identité (financières, morales, etc.) ainsi que les usages non prévus des données [(2)] (publicité ciblée, discriminations ou traitements défavorables liés au profilage, exclusion ou perte de chances – emplois, emprunts, etc. , courriels non désirés, sentiment de perte de contrôle sur ses informations personnelles, etc.).

– les préjudices liés aux disséminations d'information qui résultent de violations de confidentialité (conséquences matérielles [(3)] ou morales [(4)]) ou encore de la publication d'informations mensongères, de chantage, de diffamation, etc.

– les préjudices causés par les intrusions dans la sphère privée : les intrusions dans l'intimité de la personne [(5)], l'impossibilité de se retirer dans la solitude, les pressions avec leurs conséquences morales sur les personnes mais aussi la société tout entière [(6)]. Cette catégorie comprend également les interférences indues dans les décisions des personnes (qui portent atteinte à leur autonomie) et la manipulation.

D'autres classifications ont été proposées, chacune d'elle fournissant un éclairage différent et pouvant donner lieu à discussion. L'objectif n'est pas ici d'établir une énumération exhaustive ou définitive des préjudices liés aux atteintes à la vie privée, d'autant plus que ceux-ci sont les produits de normes sociales et donc sujets à évolution. Leur élaboration doit donc résulter d'un consensus ou pour le moins refléter les attentes de la société à un moment donné. De plus, la liste des préjudices considérés dans une analyse doit être documentée de façon à pouvoir l'adapter aux évolutions éventuelles du contexte et réviser l'analyse de risques en conséquence.

---

(1) Qui peuvent en savoir beaucoup plus sur eux que leur proches (voire qu'eux-mêmes dans certains cas).

(2) Secondary use.

(3) Par exemple les incidences financières ou l'impact sur la sécurité des personnes.

(4) Par exemple l'embarras, le discrédit, l'atteinte à la réputation, à la dignité, la perte de confiance, l'impossibilité de se défaire de son passé, etc., pour les personnes mais aussi pour la société : entrave à la liberté d'association, d'expression, etc.

(5) La sphère privée peut être délimitée ou pas par un univers spatial : domicile, ordinateur, courriels non désirés, interruptions, etc.

(6) Comme l'a rappelé notamment Daniel Solove citant Hannah Arendt, l'existence d'une sphère privée est essentielle au développement d'une vie publique de qualité.

Analyse et de gestion de risques, *accountability*

L'identification de risques de préjudices ne signifie pas forcément qu'un traitement doive être interdit ou empêché à tout prix : l'analyse de risques doit éclairer sur leur probabilité, leur gravité, et la possibilité de les réduire par le choix de contre-mesures effectives. En dernier ressort, il faut mettre les risques résiduels en regard de l'ensemble des bénéfices attendus du traitement en question. Pour que les résultats d'une analyse de risques soient les moins contestables possible, il est nécessaire que celle-ci soit effectuée sur des bases techniques rigoureuses et que toutes les hypothèses du raisonnement, ainsi que toutes les décisions reposant sur ses résultats soient traçables et justifiables.

De nombreux travaux ont eu lieu ces dernières années sur les analyses d'impact en matière de vie privée (*privacy impact assessments* [(1)]). Des progrès importants sont encore nécessaires cependant, notamment pour prendre en compte la difficile question de l'anonymisation et des risques résiduels de désanonymisation. D'un point de vue procédural et réglementaire, il serait aussi utile de promouvoir des standards d'analyse de risques dédiés à la protection de la vie privée et de susciter le développement d'un écosystème de la certification (certification des méthodes d'analyse elles-mêmes, des algorithmes d'anonymisation, et de tout produit ou système pouvant avoir une incidence sur la vie privée). En effet, même si on peut encourager tout responsable de traitement à effectuer une analyse de risques préalablement au déploiement d'un nouveau traitement informatique, il serait dangereux de laisser cette analyse à la seule appréciation d'une partie intéressée au déploiement en question : pour éviter que la démarche d'analyse de risques ne se réduise à un exercice d'auto-légitimation se traduisant *in fine* par un amoindrissement des droits des personnes [(2)] , il est primordial que la procédure puisse être effectuée ou validée par une tierce partie indépendante [(3)].

En fonction des risques identifiés, des décisions peuvent être prises quant au déploiement du système et, si celui-ci est validé, sur les contre-mesures qui doivent être mises en œuvre : d'un point de vue technique, celles-ci peuvent comprendre notamment une phase d'assainissement (anonymisation), un choix d'architecture distribuée offrant un plus grand contrôle au sujet et des limitations d'accès aux données. Mais les contre-mesures à mettre en œuvre ne sont pas exclusivement d'ordre technique : elles doivent également comporter des règles organisationnelles (gestion des habilitations, information des utilisateurs, etc.) et des précautions juridiques (accords de confidentialité, engagement de respect des mesures organisationnelles et techniques, responsabilités, etc.).

Par ailleurs, comme dans le domaine de la sécurité, un ensemble de mesures n'apporte jamais une garantie absolue de protection contre les risques. Plus encore qu'en matière de sécurité, il est difficile de prévoir l'évolution des risques d'atteinte à la vie privée. Par exemple, la capacité de désanonymisation d'un jeu de données par un tiers dépend étroitement des connaissances annexes dont peut disposer ce tiers, et la nature de ces connaissances est extrêmement difficile à prévoir à l'heure d'internet, des réseaux sociaux et

---

(1) D. Wright, P. de Hert (eds.), « Privacy impact assessment », Springer Verlag, Governance and Technology Series*, vol. 6, 2012. Etude d'Impact sur la Vie Privée (EIVP), Privacy Impact Assessment (PIA), Comment mener une EIVP, un PIA, CNIL, juin 2015* http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-1-Methode.pdf.

(2) R. Gellert, « Data protection : a risk régulation ? Between the risk management of everything and the precautionary alternative », International data privacy law, 2015, Vol. 5, N° 1.

(3) Idéalement cette partie devrait être accréditée par l'autorité de protection des données, en l'occurrence la CNIL pour la France, à l'instar de ce qui se passe dans le monde de la sécurité informatique où l'ANSSI accrédite des laboratoires d'évaluation de la sécurité des systèmes informatiques.

des objets connectés. Il est donc nécessaire de s’assurer que les dispositions nécessaires seront prises en cas de désanonymisation et que l’analyse de risques initiale sera constamment réévaluée en fonction de l’évolution des techniques et des connaissances disponibles dans une véritable démarche de prévention et de réduction permanente des risques.

C. CONTRIBUTION DE MME FRANCESCA MUSIANI : LA NOTION DE *PRIVACY BY DESIGN*

Dans le contexte de la protection des données personnelles dans les activités de partage et réseautage en ligne, le concept de *privacy* est aujourd'hui en train de présenter de nouvelles facettes, à cause des reconfigurations de la relation entre propriété et données personnelles, et de la perméabilité croissante des frontières du numérique qui ouvrent des nouvelles possibilités de surveillance de l'utilisateur/consommateur des services Internet [(1)]. En particulier et récemment, grâce notamment aux travaux de la psychologue et juriste Ann Cavoukian, une conceptualisation de la *privacy* comme principe implanté (*embedded*) dans la technologie est en train de prendre pied, sous l'étiquette de « *privacy by design* » [Cavoukian, 2006 ; 2009 ; 2010 ; Schaar, 2010]. Le PbD, pouvant se traduire en français par l'expression « la prise en compte de la vie privée dès la conception », est problématisé comme le principe techno-juridique selon lequel toute technologie exploitant les données personnelles doit intégrer la protection de la vie privée dès sa conception, et s'y conformer tout au long de son cycle de vie. C'est une forme de prévention du risque d'exploitation abusive de ces données qui se met en place, en intégrant un dispositif technique de protection juridique dès la conception des solutions informatiques destinées aux services Internet. Marc Langheinrich et Nigel Davies résument ainsi l'enjeu :

« *Aussi important qu'il soit de se référer aux lois et codes juridiques existants, qui peuvent et doivent servir de lignes guide importantes pour créer des infrastructures respectueuses de la vie privée – il est tout aussi important de se rappeler que le droit ne peut fonctionner qu'avec la réalité socio-technique, pas en opposition. Si certaines contraintes juridiques ne sont tout simplement pas exécutables, des solutions techniques et procédurales doivent être envisagées – ou le droit modifié* » [Langheinrich & Davies, 2013 : 4].

Par ailleurs, le PbD n'est pas encore adopté à large échelle, pour un ensemble de raisons qui sont en partie juridiques et économiques : le droit n'a pas de dimension contraignante au sujet, et cela démotive l'industrie à s'engager pleinement dans cette voie (ce qui pourrait par ailleurs changer avec le Règlement européen en cours d'élaboration). Mais les difficultés d'adoption du PbD tiennent aussi à la technique : comme le fait remarquer Daniel Le Métayer, le PbD se trouve actuellement à un stade où de nombreux développeurs se sont penchés sur différents instruments et méthodes d'inscription de la *privacy* dans la technologie, mais il n'existe pas de méthodologie générale pour en assurer l'implémentation.

« *Le PbD va bien au-delà des outils de protection de la vie privée : il a trait aux exigences générales d'un système, et à la définition de son architecture. Ainsi, le PbD est une question de choix : de nombreuses options sont disponibles pour servir un ensemble de fonctionnalités spécifiques – certaines d'entre elles promeuvent la privacy, d'autres moins. Il est donc nécessaire d'avoir une vision claire du système dans son ensemble, des acteurs concernés, des flux d'information* […] *afin de s'assurer qu'un ensemble d'instruments spécifiques soit en harmonie avec les exigences de* privacy » [Le Métayer, 2010, ma traduction] [(2)].

Si le concept et l'ontologie même du PbD sont donc fortement débattus [Rubinstein, 2011], des objets, des marchés, des réalités économiques commencent à se construire autour

---

(1) Ce texte est une réélaboration d'un extrait du chapitre 1 de mon livre Nains sans géants. Architecture décentralisée et services Internet, *Paris, Presses des Mines (2013, 2ème édition, 2015).*

(2) Voir aussi [Antignac & Le Métayer, 2014].

de ce concept, en entraînant l'intérêt et le suivi de la part d'instances de régulation nationales, européennes et internationales.

L'idée d'inscrire la protection de la vie privée dans les systèmes d'information n'est pas nouvelle (figurant déjà, par exemple, à l'article 17 de la Directive 95/46/CE**)** ; cependant, « *les commissaires à la protection des données personnelles ont été tout particulièrement actifs au cours des dernières années* » [Pagallo, 2012]. Le PbD est désormais proposé de plus en plus souvent – en particulier outre-Atlantique, grâce au travail d'Ann Cavoukian en tant que commissaire à la vie privée et l'information de l'Ontario – comme un principe obligatoire à intégrer dans toutes les TIC et les technologies de sécurité comme la vidéosurveillance, basées sur la collecte, l'analyse et l'échange des données personnelles. Au niveau de l'Union Européenne, la Commissaire européenne chargée de la justice, le Contrôleur Européen de la Protection des Données (CEPD) et le G29 (le groupe de travail réunissant les représentants des CNIL européennes) ont exprimé le souhait que ce concept soit intégré à la législation européenne, en tant que principe concernant toute institution ou organisation, publique ou privée, pour qui les données personnelles constituent une importante ressource fonctionnelle et stratégique [WP Article 29, 2009]. La grande occasion de porter un soutien actif à ce principe est sans doute représentée par les négociations actuellement en cours sur le projet de Règlement de protection des données en Europe [(1)]. Ce texte, qui sera amené à remplacer la Directive sur la protection des données 95/46/EC, est explicitement reconnu par l'Europe comme une nécessité face aux « *défis de la mondialisation et des nouvelles technologies* » [(2)], et introduit des références explicites (et contraignantes) au PbD.

Certains spécialistes du droit des TIC apportent depuis quelques années des éléments intéressants au débat sur la relation entre privacy et conception des dispositifs techniques, en le reliant notamment à des questions de surveillance « pervasive » et de droit de propriété. En se concentrant sur la relation entre *privacy* informationnelle et protection du droit d'auteur, Sonia Katyal arrive à une conclusion qui dépasse le cadre des *copyright wars* pour éclairer les manières dont la *privacy* s'inscrit dans les objets et architectures techniques [2004 ; 2005 ; 2009]. Nombre de stratégies d'application du droit d'auteur, toujours plus omniprésentes et invasives, ont vu le jour au cours des dernières années, et partagent le fait de fonder leur mise en œuvre et leur capacité de contrôle sur des mécanismes de surveillance « privée ». Si dans le passé, les législateurs et les spécialistes ont concentré leur attention sur d'autres méthodes de surveillance plus visibles, concernant le marketing, l'emploi ou encore la sécurité nationale, le phénomène de la « *piracy surveillance* » – les systèmes extra-judiciaires de monitorage et exécution qui identifient ou découragent les infractions de la part des consommateurs, est « *théorisé de manière incomplète, dépourvu de frontières techniques, et en puissance, incontrôlable juridiquement* » [Katyal, 2005 : 227].

Comme le soulignent Frances Grodzinsky et Herman Tavani, la surveillance et les manières d'échapper à la surveillance sont actuellement au centre des débats au croisement entre *privacy*, propriété et expression sur les réseaux parce que, quand la charge d'y identifier les infractions a été placée sur les détenteurs de droits d'auteur, cela a légitimé en quelque sorte la montée en puissance « *d'une industrie entièrement nouvelle où les propriétaires de contenus ont le droit de* [mobiliser des dispositifs techniques afin de] *parcourir l'Internet à la recherche de potentiels contrefacteurs* » [Grodzinsky & Tavani, 2005 : 247] ; montée en puissance qui s'étend aux agences de renseignement, comme les révélations Snowden l'ont montré. Cette « nouvelle » surveillance contribue à faciliter et à rendre omniprésents les enregistrements des activités des consommateurs, y compris celles

---

(1) http://ec.europa.eu/justice/data-protection/index_fr.html.

(2) Ibid.

qui ne constituent pas une violation ; à imposer des standards d'usage et d'expression ; à réduire ou à proscrire des activités considérées comme inacceptables. La dialectique entre le droit à la vie privée et l'ensemble des activités quotidiennes en réseau montre le besoin de résoudre les tensions entre vie privée et présence active sur les réseaux de façon qui protège la relation entre les nouvelles technologies et les libertés personnelles de manière dynamique et plurielle, par le droit autant que par la technique [Katyal, 2004].

C'est dans cette perspective que s'inscrivent les travaux de Niva Elkin-Koren [2002 ; 2006 ; 2012]. Selon la juriste israélienne, la relation entre loi et technique se focalise trop souvent sur un aspect en particulier, les défis que les technologies émergentes posent aux régimes légaux existants, créant dès lors un besoin de réforme de ces mêmes régimes légaux. Les mesures juridiques qui concernent la technique à la fois comme cible de régulation et instrument d'exécution devraient, par ailleurs, considérer que la loi ne répond pas simplement aux nouvelles technologies, mais contribue à les façonner et en influence le design, tout comme le design peut influencer voire se substituer parfois à la loi [Elkin-Koren, 2006 : 15]. Les systèmes de surveillance technique et juridique qui n'implémentent pas cet aspect vont probablement influencer l'innovation technique de manière à empêcher ou limiter ses bénéfices socio-économiques potentiels (*ibid.*, 21), ou sacrifier les principes fondamentaux de la *privacy* informationnelle au bénéfice d'une capacité de contrôle dépourvue de limites [Katyal, 2004; 2005].

En conclusion, la *privacy* de l'information et des données personnelles en réseau peut être définie et conceptualisée – ainsi qu'assurée ou entravée – au moyen de différentes modalités de traitement et de gestion technique des données, et selon différentes priorités dérivant de la concurrence entre droits, des évolutions des usages, et de la mise en œuvre de technologies de surveillance et contre-surveillance. Comme l'a récemment souligné une séance dédiée de l'*European Data Governance Forum* (siège de l'UNESCO, Paris, 8 décembre 2014) [(1)], si les technologies de l'information et de la communication posent aujourd'hui des questions toujours renouvelées aux régulateurs en matière de protection de la vie privée et de sécurité des données, les choix technologiques – de design, de conception, d'implémentation – sont eux-mêmes devenus des éléments centraux dans la protection des individus, sur lesquels le droit et la régulation s'appuient désormais de façon croissante.

Références

[Antignac & Le Métayer, 2014] Antignac, T & Le Métayer, D (2014). Privacy by design : from technologies to architectures – (position paper). In Annual privacy forum (APF 2014), Volume 8450 of the lecture notes in computer science, pp. 1-17, Springer.

[Cavoukian, 2006] Cavoukian, A. (2006). Privacy by Design : The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. https://www.privacyassociation.org/media/presentations/11Summit/RealitiesHO1.pdf.

[Cavoukian, 2009] Cavoukian, A. (2009). "Privacy by Design". The Answer to Overcoming Negative Externalities Arising From Poor Management of Personal Data. Trust Economics Workshop, Londres, 23 juin 2009.

[Cavoukian, 2010] Cavoukian, A. (eds., 2010) Special Issue: Privacy by Design: The Next Generation in the Evolution of Privacy. Identity in the Information Society, 3(2).

(1) *http://europeandatagovernance-forum.com/pro/fiche/quest.jsp;jsessionid=vzlmQy7FxI4aJj5mpLR0iwLT.gl2?pg=programme*.

[Elkin-Koren, 2002] Elkin-Koren, N. (2002). It's All About Control: Rethinking Copyright in the New Information Landscape. In Elkin-Koren, N. & Netanel, N. W. (eds.) The Commodification of Information, Kluwer Law International, The Hague.

[Elkin-Koren, 2006] Elkin-Koren, N. (2006). Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic. New York University Journal of Legislation & Public Policy, 9 (15), 15-76.

[Elkin-Koren, 2012] Elkin-Koren, N. (2012). Governing Access to User-Generated Content: The Changing Nature of Private Ordering in Digital Networks. In Brousseau, E., Marzouki, M., Méadel, C. (eds.), Governance, Regulations and Powers on the Internet, Cambridge: Cambridge University Press.

[Grodzinsky & Tavani, 2005] Grodzinsky, F. S. & Tavani, H. T. (2005). P2P Networks and the Verizon v. RIAA Case: Implications for Personal Privacy and Intellectual Property. Ethics and Information Technology, 7, 243-250.

[Katyal, 2005] Katyal, S. (2005). Privacy Vs. Piracy. Yale Journal of Law and Technology, 7, 222-345.

[Katyal, 2009] Katyal, S. (2009). Filtering, Piracy Surveillance, and Disobedience. Columbia Journal of Law & the Arts, 32 (4) : 401-426.

[Langheinrich & Davies, 2013] Langheinrich, M., & Davies, N. (2013). Privacy By Design. IEEE Pervasive Computing, 12 (2) : 2-4.

[Le Métayer, 2010] Le Métayer, D. (2010). Privacy by design : a matter of choice in Data protection in a profiled world. Serge Gutwirth, Yves Poullet, Paul De Hert (eds.), pp. 323-334, Springer.

[Pagallo, 2012] Pagallo, U. (2012). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In S. Gutwirth et al. (eds.) European Data Protection: In Good Health? Berlin : Springer.

[Rubinstein, 2011] Rubinstein, I. S. (2011). Regulating Privacy By Design, Berkeley Technology and Law Journal, 26.

[WP Article 29, 2009] Working Party (WP) Article 29 D-95/46/EC. 2009. The future of privacy. 02356/09/EN–WP 168.

D. CONTRIBUTION DE M. CYRIL ZIMMERMANN : LA NOTION D'*ACCOUNTABILITY*

L'***accountability*** est une forme importante de protection permettant d'exiger d'un opérateur privé qu'il rende des comptes sur la manière dont il a collecté des données, l'utilisation qu'il en a faite et les moyens mis en œuvre pour les conserver de manière satisfaisante. Cette exigence doit se doter d'un environnement juridique, politique et social renouvelé et crédible. En effet, il ne s'agit pas seulement d'obtenir des informations et un surplus de transparence de la part d'opérateurs publics mais aussi privés. Il s'agit notamment de fixer des règles et un cadre à sociétés commerciales qui sont en train de créer de nouveaux ensembles sociaux, parfois des sous-ensembles, parfois des intersections d'ensembles préexistants. Qu'ils aient eu comme point de départ la création d'une galerie marchande, d'un moteur de recherche ou d'un réseau social porté par des applications ludiques, ces opérateurs privés à la puissance considérable façonnent des espaces sociaux numériques. Ils créent et gèrent quasiment en dehors de tout contrôle des espaces qui ne sont pas tout à fait publics mais atteignent de telles dimensions qu'ils ne peuvent pas être considérés comme totalement privés non plus.

Nous assistons en effet à la définition de rapports inédits entre l'individu et des organisations commerciales extrêmement puissantes qui gèrent des données personnelles à une échelle sans précédent. Ces données sont agrégées et traitées par des algorithmes tellement puissants qu'ils peuvent créer et organiser des rapports sociaux entre des individus au même titre que la puissance publique le fait depuis la création des États modernes. Par exemple, les réseaux sociaux peuvent créer du lien social par le partage très large d'informations personnelles, par la mise en relation non spontanée entre individus, par la stimulation de la diffusion de l'information ou par la hiérarchisation des informations publiées. Ce lien est censé répondre aux désidératas non formulés de chacun mais peut aussi relever de la manipulation si un biais commercial non clairement affiché vient le déterminer. Aussi, il serait paradoxal de vouloir renouveler l'encadrement de l'action de l'État et de son administration à l'ère du numérique sans prendre en considération les nouveaux acteurs qui constituent des menaces potentielles pour les libertés publiques.

Il convient donc de se préoccuper très pragmatiquement de la puissance et du rôle de ces opérateurs privés d'espaces sociaux numériques, alors qu'ils utilisent aujourd'hui le *big data* à des fins de profilage de chaque utilisateur d'une manière qu'aucune organisation, aucun État ou aucun régime politique n'a jamais pratiqué ou même envisagé. Il appartient aux pouvoirs publics de transformer ces espaces sociaux, notamment par la mise en pratique de la notion d'« *accountability* » vis-à-vis des opérateurs privés, en véritables sociétés numériques dotées de règles de savoir-vivre ensemble digital.

Il nous paraît que pour permettre une mise en application réelle du principe d'« *accountability* », il convient en premier lieu de revisiter le cadre juridique auquel sont soumis les opérateurs privés de ces nouveaux espaces sociaux numériques, également appelés « plateformes », pour confirmer que notre droit peut vraiment s'appliquer à eux. Ce droit devrait poser comme principe que la territorialité du traitement dépend du lieu de résidence et/ou de la nationalité de l'utilisateur (1) et que cet échange doit suivre des règles de transparence quant aux algorithmes utilisés (2). Il convient ensuite de doter le régulateur ou l'autorité judiciaire de véritables moyens qui lui donnent crédibilité et pouvoir d'action (3). Le cadre ainsi mis en place devra être complété par le contre-pouvoir que peut constituer la coalition de citoyens numériques. Ils devront être informés et éclairés sur le contexte, les enjeux et les choix politiques déjà formulés (4) pour ensuite utiliser des outils d'action collective juridiquement reconnus (5).

1. Les pratiques des opérateurs privés sont aujourd'hui difficilement contrôlables car elles se déploient dans des espaces sociaux sans territorialité

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés se réfère à la situation géographique du responsable du traitement ou du moyen de traitement en lui-même et non de l'utilisateur. L'article 5 de la loi dispose ainsi : « *I. - Sont soumis à la présente loi les traitements de données à caractère personnel : 1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ; 2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne* ».

Ces critères d'applicabilité semblent aujourd'hui particulièrement inadaptés à appréhender les traitements réalisés par les opérateurs privés dans le cadre d'espaces sociaux qui ne se limitent pas aux frontières d'un territoire ou d'un ensemble géographique déterminé. La délibération du 3 janvier 2014 (D2013-420) de la Commission nationale de l'Informatique et des Libertés (CNIL) à l'encontre de la société *Google Inc*, en constitue une parfaite illustration, l'applicabilité de la loi informatique et Libertés et la compétence de la CNIL ayant été abondamment questionnées par cet opérateur. La Commission a procédé par interprétation pour parvenir à rendre sa décision et motiver l'existence de moyens de traitement sur le territoire Français, considérant notamment l'activité d'intermédiation publicitaire réalisée par la structure *Google France* et basée sur le résultat des traitements de *Google Inc*, ainsi que la présence d'un moyen de traitement représenté par les cookies déposés sur les terminaux des utilisateurs Français.

Cette interprétation, bien qu'ayant permis d'appliquer la loi, n'est pas suffisante pour englober l'ensemble des espaces sociaux créés par les opérateurs privés et prendre en compte les évolutions de la technique. Tous les opérateurs privés ne disposent pas d'une structure publicitaire implantée en France et ne fonctionnent pas nécessairement avec des cookies. La situation des *cookies* est aujourd'hui particulièrement précaire et le cadre législatif qui leur est applicable peine à s'imposer face à la complexité des réseaux et aux impératifs d'instantanéité des échanges. L'incertitude créée par la trop grande place de l'interprétation des critères d'applicabilité de la loi doit également être soulignée. Si la place de l'interprétation ne fait pas obstacle à une décision comme celle qui a été rendue par la CNIL dans un environnement dans lequel les sanctions encourues sont limitées (comme celui que nous connaissons aujourd'hui), il n'est pas certain qu'il en soit de même dans un environnement dans lequel la sanction présente un caractère beaucoup plus contraignant. Or, il est nécessaire de renforcer les sanctions encourues en cas d'infraction à la loi afin de garantir sa légitimité et sa force contraignante. La réponse de la loi doit être proportionnée à l'étendue des espaces sociaux et des atteintes à la vie privée qu'ils peuvent générer.

La situation de déséquilibre créée par une loi qui n'est plus adaptée à son époque, dans ses sanctions comme dans ses critères d'applicabilité représente une menace grandissante pour les citoyens comme pour les pouvoir publics. Elle contribue, en outre, à créer une distorsion entre les opérateurs privés. Il convient de faire évoluer cette situation afin de mieux protéger les libertés de chacun. La première étape serait d'imposer une notion de territorialité au service, liée au lieu de résidence et/ou à la nationalité de l'individu ou encore au fournisseur d'accès utilisé lors de l'inscription. Il est également envisageable de laisser à l'utilisateur le choix de l'autorité et du droit auquel il souhaite confier la protection de ses données.

Il appartiendrait des lors à chacun de choisir se placer sous la protection de son droit national ou du droit qu'il a choisi pour gérer ses relations avec la plate-forme. Le respect des conceptions locales des libertés publiques pourrait ainsi être assuré devant la justice locale sans incertitude sur l'applicabilité de la Loi, offrir une meilleure compréhension des droits et obligations réciproques et une plus grande protection de chaque individu. De même des autorités de régulation comme la CNIL seraient fondées à agir « automatiquement » pour faire des contrôles réguliers des bonnes pratiques des plates-formes. Elle deviendrait ainsi une force de dissuasion plus efficace pour faire respecter le droit. Cette évolution des critères d'application de la loi permet en outre d'ouvrir le débat sur une aggravation des sanctions encourues.

2. Un principe : une transparence de l'algorithme et des règles

Au-delà de collecter des données personnelles, les opérateurs des espaces sociaux numériques les exploitent d'une façon inédite grâce à la mise en place d'algorithmes puissants. À partir d'informations collectées au fil de l'utilisation des services par un internaute, ces algorithmes permettent d'extrapoler de nouvelles informations sans lien évident avec celles que l'internaute a « exporté » ou cédé à la plateforme.

L'exemple des « *look-alike* » des plateformes marketing utilisant le *big data* est assez éclairant : il est possible de rapprocher d'un échantillon de personnes A dont on a recueilli l'intérêt pour un sujet ou un objet O, un groupe de personnes B ou C qui ont des profils comparables aux individus composant A sur toute une série de critères mais dont ne connaît pas l'intérêt pour O. On pourra tester l'intérêt de B et de C pour 0 via des campagnes de publicité et en déduire lequel de ces 2 groupes est la cible marketing idéale la plus proche de A.

Il est donc possible à partir d'une connaissance assez fine des goûts et préférences d'un groupe d'individu relativement limité, et d'un stockage systématique de toutes les informations concernant les autres individus d'extrapoler de proche en proche des profils de goût et de préférence de tous les individus qui sont inscrits et qui utilisent une plateforme de services numériques. Est-il acceptable que sans que nous en ayons conscience, sans qu'on nous l'explique *ab initio*, sans qu'on nous informe de chaque étape du processus en nous laissant le choix de s'y opposer, un acteur économique puisse construire un profil statistique de nos goûts, de nos préférences, de ce que nous consommons, de la période de notre vie de consommateur dans laquelle nous nous trouvons ? Sans doute une partie de ce que nous consommons appartient à notre vie privée. Et nous nous opposerions au partage de cette information si la question nous était clairement posée. Par ailleurs, sommes-nous conscients du tri et donc de la manipulation l'information reçue par les internautes pour mieux orienter leur intérêt vers des sujets dont l'intérêt commercial est plus évident pour l'acteur économique qui opère l'espace social numérique ? Et si demain cet opérateur économique prenait des options politiques lui permettant de définir au mieux ses intérêts économiques, quel contrôle pourrions-nous exercer sur les tris, manipulations d'information et extrapolations de nos goûts et préférences auquel il nous soumet ?

Aujourd'hui il est impossible de contrôler efficacement ces plateformes et les opérations auxquelles elles se livrent. La manière la plus rapide de le permettre serait de leur demander de rendre public leur algorithme de traitement de l'information de façon à ce que la communauté des internautes (seule puissance capable aujourd'hui de l'analyser en temps réel) puisse observer ses démarches et avertir les internautes. Le risque de réputation et de rejet des utilisateurs semble aujourd'hui le garde-fou le plus efficace contre l'*hybris* des plateformes globales et les menaces qu'elles peuvent représenter pour les libertés publiques.

Mais si le principe de territorialité précédemment évoqué s'applique, les opérateurs seront soumis au droit local dans l'usage qu'ils font des données personnelles et le régulateur pourra également surveiller leurs algorithmes rendus publics, avertir lui aussi les internautes et si besoin interdire certains traitements de données.

3. Une application par un renforcement des moyens

Pour que le régulateur puisse remplir son nouveau rôle, conçu comme plus ambitieux que ce qu'il a été jusqu'à présent, le renouvellement du cadre juridique tel qu'évoqué est une étape indispensable mais il est évidemment nécessaire de renforcer les moyens dont il dispose.

Le fait que l'univers digital soit global ou et opéré par des acteurs économiques agissant à partir de centres de décision placés en dehors du territoire national ou de l'espace européen ne doit pas servir d'excuse à l'inaction. Il en était de même il y a 30 ans avec la libéralisation de la finance de marché, avec le développement des mécanismes d'ingénierie financière assistés par les outils informatiques et le déploiement d'acteurs internationaux gérant des sommes supérieures au budget d'un État. Cela n'a pas empêché la mise en place d'autorités de surveillance et de contrôle des marchés financiers. Au contraire chaque nouvelle étape de sophistication et de gain de puissance des acteurs de la finance de marché justifie de nouveaux moyens pour les autorités boursières. Ceux-ci, bien qu'encore insuffisantes, ont permis au régulateur financier d'édicter des règles de conduite et de sanctionner les opérateurs nationaux ou internationaux qui ne s'y confirment pas. Les autorités américaines ont d'ailleurs récemment décidé d'amendes de plusieurs milliards d'euros envers des banques étrangères qui opéraient sur le sol américain ou traitaient en devises américaines.

Les similitudes entre l'industrie financière et l'industrie digitale en termes de rapidité de développement des acteurs économiques à encadrer, de l'apparente inégalité du rapport de force financier et géographique entre régulateur et opérateurs privés, permettent de penser que si les pouvoirs publics prennent conscience des enjeux, ils peuvent doter nos sociétés de moyens de protection dont l'efficacité ne sera certes pas totale mais a été jugée un minimum nécessaire par ailleurs.

Les espaces sociaux numériques seraient donc à la fois encadrés par la loi, surveillés par la communauté des internautes et informaticiens les plus actifs, ainsi que contrôlés ou arbitrés par un régulateur ou un juge qui dispose des moyens nécessaires à son action. Borner ainsi les actions de chacun et des groupes d'intérêt est une étape nécessaire mais point suffisante. Il convient d'éclairer chaque citoyen numérique sur le cadre légal, sur ses droits, sur ses devoirs et sur les enjeux du vivre ensemble digital.

4. Une nécessaire pédagogie

Favoriser la pédagogie sur la gestion des données

La liberté individuelle à l'heure d'internet doit être conquise et défendue, et la possibilité de maîtriser notre vie en ligne également. Il peut être intéressant de profiter des révélations de l'affaire Snowden et des réactions des opinions publiques pour créer et initier une nouvelle forme de pédagogie, une nouvelle forme de sensibilisation à la gestion des données personnelles. On pourrait imaginer par exemple confier à la CNIL et aux autres autorités de gestion de l'économie numérique et de l'ère numérique plus généralement une mission pédagogique, en parallèle ou en partenariat avec le « Brevet Informatique et Internet » (B2I), qui pourra être étendu aux droits et libertés et aux notions fondamentales du « monde numérique », incomprises du grand public.

Agir en concertation avec les citoyens

Par la pédagogie et l'information, il est indispensable de renforcer la place de l'individu dans le système juridique. La protection de la vie privée est bien évidemment un droit fondamental et doit le rester. À l'ère du numérique, il est néanmoins indispensable de repenser l'application de ce droit. La protection des données à caractère personnel -, doit être assurée dans l'intérêt des citoyens, mais également en relation avec eux, puisqu'ils doivent pouvoir choisir le devenir de leurs données et donc être informés des choix dont ils disposent :

- laisser l'exploitation aux opérateurs économiques des espaces sociaux numériques, mais pour quelle contrepartie ?
- interdire toute exploitation de ses données personnelles, mais pour quelle qualité de prestation ou de service ?
- être capable de récupérer toutes ses données personnelles pour les exporter dans un autre espace social numérique ? Avec quel degré de contrôle ?
- monnayer l'utilisation de ses données ? mais avec quelle capacité de contrôle et quel espoir de gain ?

Il convient d'ouvrir ces débats pour informer, expliquer et éclairer les choix politiques qui ont été faits à ce jour (un utilisateur ne monnaye pas ses données personnelles et l'État est garant de leur intégrité et protection) et ceux qui pourraient être faits demain.

Bénéficiant d'un cadre législatif adapté à la réalité digitale et d'un régulateur crédible, les citoyens numériques raisonnablement éclairés peuvent et doivent également devenir un des maillons de la défense des libertés publiques. Il convient de leur donner les moyens d'agir.

5. Ouvrir la possibilité d'actions collectives (*class actions*, votations)

Il faut donner une visibilité et une place importante à la vigilance et aux manifestations de résistance spontanée des groupes d'utilisateurs attachés à la défense des libertés publiques. Il s'agit d'encourager l'utilisation des espaces sociaux numériques et de leurs outils de communication virale pour diffuser des initiatives de défense des libertés publiques contre les menaces et agressions potentielles dont l'opérateur économique peut se rendre coupable.

Lanceurs d'alertes d'un nouveau genre, individus isolés utilisant la puissance communautaire des réseaux sociaux ou groupes organisés avec un rôle affirmé de gardien des libertés publiques, ils doivent pouvoir bénéficier d'une capacité d'action judiciaire renforcée. En cela ils seraient mis sur le même plan que les associations de consommateurs qui introduisent des actions collectives (*class actions*). Il serait sans doute souhaitable d'aller au-delà de l'action judiciaire et de donner à ces mouvements « citoyens » la possibilité de proposer des lois à la représentation nationale. Un système de votation électronique permettrait de recueillir des propositions de texte protégeant les libertés publiques et de les soumettre à une approbation électronique. Ainsi, une initiative numérique populaire qui atteint un certain nombre de votes favorables, serait ensuite proposée à l'agenda parlementaire.

Les espaces sociaux numériques ne seraient donc plus de nouveaux « *far west* » ou l'individu ou l'opérateur économique du réseau pourrait menacer les libertés publiques de chacun. Grâce à une action législative, politique et sociale considérablement rénovée et adaptée aux enjeux, le principe d'*accountability* pourrait devenir un instrument concret et crédible de défense des libertés publiques.

IV. LISTE DES 100 RECOMMANDATIONS

I. RENFORCER LE DROIT À L'INFORMATION À L'ÈRE NUMÉRIQUE

A. CONSACRER UN DROIT FONDAMENTAL À L'INFORMATION D'INTÉRÊT PUBLIC

Recommandation n° 1

Instaurer un droit fondamental à l'information d'intérêt public ouvert à tout individu et fondé sur une présomption de libre communicabilité des informations publiques.

Transformer les compétences et les prérogatives de l'actuelle Commission d'accès aux documents administratifs (CADA) pour en faire un service indépendant chargé de veiller à la bonne application de ce droit, doté de pouvoirs décisionnels, sur le modèle de l'Information Commissioner britannique.

Recommandation n° 2

Élargir la catégorie des documents communicables à certains documents préparatoires ou préalables à la décision d'une autorité publique.

Recommandation n° 3

Moduler la confidentialité attachée aux informations à caractère personnel lorsqu'elles présentent un intérêt public important.

Recommandation n° 4

Mieux concilier l'exigence de protection de la vie privée avec l'impératif d'ouverture et de réutilisation des données publiques, y compris lorsque ces dernières sont susceptibles de se rapporter ultérieurement à une personne identifiée, en mettant en place une doctrine de protection des données personnelles limitant au maximum les risques de réidentification.

Recommandation n° 5

Afin de renforcer la transparence du fonctionnement des services publics, élargir la catégorie des documents communicables par les services publics industriels et commerciaux (transports, eau, déchets, énergie, etc.).

Recommandation n° 6

Encourager les entreprises et les organismes fournissant des services considérés comme essentiels ou bénéficiaires de subventions publiques (télécommunications, logement, sport, culture, etc.) à communiquer les documents et les données d'intérêt général qu'ils détiennent.

B. ORGANISER LE DROIT À L'INFORMATION PUBLIQUE À L'ÈRE NUMÉRIQUE

Recommandation n° 7

Prioritairement à leur communication sur demande et à titre individuel, généraliser la mise en ligne des documents et informations d'intérêt public dans des conditions en garantissant l'accessibilité, la mise à jour et l'intelligibilité.

Recommandation n° 8

Conserver un droit d'accès individuel « à la demande » pour les situations dans lesquelles la mise en ligne est impossible ou manifestement trop coûteuse et mieux accompagner l'individu dans ses démarches (élaboration de guides en ligne, création de points d'accueil des demandes de communication).

Recommandation n° 9

Instaurer une obligation légale d'ouverture des données publiques. Afin de satisfaire dans les meilleures conditions à cette nouvelle obligation, préparer l'ouverture généralisée des données publiques et diffuser la culture de l'*open data* au sein des administrations concernées, en inscrivant notamment dans la loi le statut et les missions de l'administrateur général des données.

Recommandation n° 10

Inscrire dans la loi le principe de la libre réutilisation des données publiques, grâce à l'utilisation de formats de bases de données et de licences de réutilisation ouverts.

Recommandation n° 11

Inscrire dans la loi le principe selon lequel la réutilisation des données publiques s'opère à titre gratuit, sauf dans les cas, exceptionnels et dûment justifiés, pour lesquels l'établissement d'une redevance est nécessaire.

C. RENFORCER LA PROTECTION DES LANCEURS D'ALERTE

Recommandation n° 12

Élargir le champ du « droit d'alerte » aux faits manifestement contraires à l'intérêt général ou qui font peser sur sa préservation une menace grave et réelle justifiant qu'ils soient portés à la connaissance du public.

Recommandation n° 13

Instaurer un canal d'information sécurisé au profit des lanceurs d'alerte leur permettant de saisir une personnalité indépendante chargée de les protéger contre d'éventuelles menaces ou représailles. Cette personnalité pourrait être l'autorité administrative indépendante chargée de mettre en œuvre le droit à l'information publique si elle dispose d'une indépendance incontestable et de pouvoirs suffisants ou, à défaut, le Défenseur des droits.

*

* *

II. DÉFENDRE LA LIBERTÉ D'EXPRESSION

A. AFFIRMER LE PRINCIPE DE NEUTRALITÉ TECHNOLOGIQUE

Recommandation n° 14

Afin de mettre fin à l'opinion répandue selon laquelle le champ de la loi de 1881 sur la liberté de la presse se limiterait à la presse, la renommer « loi sur la liberté d'expression ».

Recommandation n° 15

Ne pas étendre à internet le régime dérogatoire extra-judiciaire d'encadrement de la liberté d'expression spécifique à l'audiovisuel.

Recommandation n° 16

Faire respecter le principe de neutralité technologique dans la définition de la politique publique de soutien à la presse, ce qui implique en particulier de défendre l'application d'un même taux de TVA, quel que soit le support.

Recommandation n° 17

Ne pas faire par principe de l'utilisation d'internet une circonstance aggravante.

Recommandation n° 18

Réaffirmer la possibilité de recourir au pseudonymat sur internet.

B. PRÉSERVER LA LOI DU 29 JUILLET 1881 SUR LA PRESSE, PILIER DE LA DÉMOCRATIE, AUJOURD'HUI MENACÉE

Recommandation n° 19

Réintroduire le délit d'apologie du terrorisme parmi les infractions relevant de la loi de 1881 sur la liberté de la presse.

Recommandation n° 20

Mettre un terme au transfert dans le code pénal des infractions à la liberté d'expression relevant de la loi de 1881sur la liberté de la presse.

Recommandation n° 21

Ne pas « réserver » les principes protecteurs de la liberté d'expression aux journalistes professionnels.

C. CONFORTER LA PLACE DU JUGE COMME GARANT DE LA LIBERTÉ D'EXPRESSION

Recommandation n° 22

Réaffirmer la dichotomie entre éditeur et hébergeur et réaffirmer la responsabilité limitée de l'hébergeur, garante de la liberté d'expression et de la liberté d'innovation.

Ne pas créer de catégorie intermédiaire des « plateformes » entre l'hébergeur et l'éditeur.

Recommandations n°s 23 à 25

– **n° 23** : substituer dans la législation la notion plus objective de « manifestement illégal » à celle de « manifestement illicite » ;

– **n° 24** : introduire le principe du contradictoire dans le retrait de contenus illégaux. Faire intervenir la plateforme PHAROS afin que l'hébergeur ne soit plus seul juge du « manifestement illicite » ;

– **n° 25** : assurer la transparence des suppressions de contenus par les hébergeurs à travers la mise en place d'une base de données des notifications et retraits en format libre et ouvert.

Recommandation n°s 26 et 27

– **n° 26** : ne pas renforcer par la loi les obligations de surveillance des intermédiaires techniques ;

– **n° 27** : réserver au juge la faculté de prononcer des injonctions de retrait prolongé de contenus illégaux.

Recommandation n° 28

N'autoriser le blocage qu'à titre subsidiaire et sur décision judiciaire.

Accompagner tout dispositif de blocage d'un dispositif d'évaluation de son efficacité.

Recommandation n° 29

Ne pas introduire de nouveau cas de blocage sur décision administrative.

Recommandation n° 30

Limiter les cas de contournement du juge par des autorités administratives.

Recommandations n°s 31 à 37

– **n° 31** : organiser un traitement prioritaire par le parquet des plaintes portant sur des contenus particulièrement odieux (en particulier les contenus d'apologie du terrorisme et de provocation au terrorisme) ;

– **n° 32** : évaluer l'opportunité de désigner un juge spécialisé, au besoin de proximité, habilité à traiter ces plaintes et/ou instaurer la possibilité pour l'autorité

administrative de saisir le juge des référés en cas de contenus manifestement odieux (diffusion d'actes de barbarie, meurtres, tortures en ligne, etc.) ;

– **n° 33** : examiner la possibilité de mettre en place une procédure judiciaire accélérée pour les simples réplications de contenus déjà condamnés ;

– **n° 34** : mettre à l'étude un dispositif inspiré du système de signalement mis en œuvre par l'Autorité de régulation des jeux en ligne (ARJEL), qui permettrait à l'autorité administrative de présenter à dates régulières à l'autorité judiciaire des séries de contenus particulièrement odieux à bloquer ;

– **n° 35** : créer un parquet spécialisé sur les questions de contenus illicites en ligne ;

– **n° 36** : créer un « pôle de compétences numériques » au sein du ministère de la Justice dédié à la mise en œuvre d'une politique pénale en la matière et au suivi des travaux européens et internationaux relatifs à la criminalité en ligne. Ce service pourrait aussi avoir un rôle d'expertise et de conseil auprès des magistrats en poste en juridiction ;

– **n° 37** : créer une filière de formation ad hoc des juges au numérique : créer des modules spécifiques dans les formations initiale et continue.

Recommandation n° 38

Améliorer l'effectivité de la loi de 1881 sur la liberté de la presse :

– préciser et actualiser les notions d'espace public et d'espace privé, au regard des nouvelles formes de communautés et de réseaux numériques du web 2.0 ;

– envisager la numérisation des procédures, notamment des assignations et significations ; simplifier et faciliter les procédures de référé par la création d'un référé numérique et prévoir la possibilité de déposer plainte en ligne ;

– prévoir un droit de réponse effectif sur internet au profit des associations antiracistes.

Recommandations n°s 39 à 41

– **n° 39** : prévoir l'application à tout hébergeur dirigeant ses activités vers la France des obligations de coopération avec les autorités administratives et judiciaires prévues par l'article 6 de la LCEN ;

– **n° 40** : réformer le MLAT (*Mutual Legal Assistance Treaty*) qui permet à l'autorité judiciaire française d'accéder à des informations stockées dans des plateformes hébergées aux États-Unis dans le but de favoriser une plus grande rapidité dans l'échange des données ;

– **n° 41** : entreprendre une action diplomatique forte pour faire signer et ratifier par les États hébergeant des sites diffusant des discours de haine le protocole additionnel n° 189 à la Convention cybercriminalité du Conseil de l'Europe spécifiquement dédié au racisme et à l'antisémitisme.

Recommandations n°s 42 à 46

– **n° 42** : organiser la simplification et la standardisation des différents dispositifs de signalement et de notification développés par les plateformes de manière totalement désordonnée ;

– **n° 43** : renforcer et généraliser les dispositifs de *fast track* accordés aux associations ;

– **n° 44** : obtenir des obligations de traitement dans des délais donnés pour les signalements opérés par les internautes auprès des plateformes ;

– **n° 45** : donner plus de visibilité à la plateforme PHAROS auprès des particuliers, notamment dans les interfaces des plateformes ;

– **n° 46** : augmenter les moyens humains, techniques et matériels de la plateforme de signalement PHAROS.

*

* *

III. REPENSER LA PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES À CARACTÈRE PERSONNEL

A. RÉÉVALUER L'IMPORTANCE DES DROITS AU RESPECT DE LA VIE PRIVÉE ET À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Recommandation n° 47 ***(pas d'unanimité)***

Inscrire explicitement dans la Constitution le droit au respect de la vie privée et l'exigence de protection des données à caractère personnel afin de réévaluer l'importance accordée à ces libertés fondamentales en droit interne.

Recommandation n° 48

Retenir une interprétation large de la notion de donnée à caractère personnel afin d'y inclure l'ensemble des données, traces, éléments ou informations personnels directement ou indirectement identifiants ou qui permettent de singulariser ou de discriminer un individu parmi d'autres, y compris les données pseudonymes.

Recommandation n° 49

Afin de réduire les risques de réidentification, promouvoir le recours à des techniques d'anonymisation robustes dans le contexte d'analyses de risques rigoureuses et valoriser les meilleures méthodes, par exemple sous la forme de labels. Les techniques d'anonymisation disponibles actuellement étant insuffisantes, renforcer l'effort de recherche dans ce domaine.

Recommandation n° 50

Encourager la conception et l'utilisation de technologies permettant de rendre effectif le principe de minimisation de la collecte de données personnelles et donnant à tout individu une réelle maîtrise sur l'utilisation de ses données (*privacy by design* et *privacy by default*) par la mise en place de dispositifs plus contraignants ou réellement incitatifs à destination des responsables de traitements et des fournisseurs de technologies et par l'instauration d'un schéma de certification de ces technologies.

Recommandation n° 51

Dans le respect des compétences de l'autorité judiciaire en matière de lutte contre les activités et contenus illégaux, inciter au recours à des technologies de chiffrement des données afin de renforcer la confidentialité des communications.

Recommandation n° 52

Mettre les architectures et les modèles d'organisation des réseaux numériques au service de la protection de la vie privée ; renforcer les obligations de sécurité à la charge des acteurs de l'internet assumant des fonctions d'intermédiation ; généraliser l'obligation de notification des failles de sécurité.

Recommandation n° 53

Passer d'une logique formelle de déclaration à une logique de mise en conformité et de respect en continu de la réglementation ;

En contrepartie, accroître la responsabilisation des exploitants de traitements de données personnelles par la généralisation des obligations de rendre compte des traitements effectués sur les données personnelles ou qui peuvent avoir une incidence sur la vie privée des individus (*accountability*) et la mise en place de procédures d'audits par des tiers indépendants ; prévoir une sensibilisation à ces questions, notamment par un renforcement de la formation continue délivrée sur ce sujet.

Recommandation n° 54

Soumettre à des obligations particulières les responsables de traitements de données personnelles exposant l'individu à des risques ou à des préjudices particuliers. À cet effet, rendre obligatoire l'analyse de risques préalable permettant d'identifier ces risques et préjudices.

Recommandation n° 55

Revoir la nature des sanctions applicables aux responsables de traitements contrevenant à la réglementation :

– augmenter significativement le montant des sanctions pécuniaires que l'autorité de protection peut prononcer à leur encontre ;

– encourager la décision de publication des sanctions consécutives aux constats d'infractions établis à leur encontre.

Recommandation n° 56

Faire du futur règlement général européen sur la protection des données une loi de police permettant l'application impérative de ses dispositions indépendamment de la loi applicable en vertu d'une clause contractuelle du responsable du traitement.

Recommandation n° 57

Pour les traitements de données implantés dans plusieurs États, coordonner à l'échelle européenne l'intervention des autorités de protection par l'institution d'un « guichet unique » respectueux du principe de proximité du citoyen avec l'autorité de protection des données ou le juge national dont il dépend.

B. DONNER À L'INDIVIDU L'AUTONOMIE INFORMATIONNELLE ET DÉCISIONNELLE NÉCESSAIRE À SON LIBRE ÉPANOUISSEMENT DANS L'UNIVERS NUMÉRIQUE

Recommandation n° 58

En complément de la reconnaissance constitutionnelle des droits au respect de la vie privée et à la protection des données personnelles, consacrer dans notre législation un droit à l'autodétermination informationnelle donnant sens aux droits reconnus à l'individu sur les réseaux numériques.

Recommandation n° 59

Passer d'une logique formelle de consentement préalable à une logique de recueil d'un consentement adapté au contexte de la collecte et du traitement des données personnelles (contexte, usages, rapports de force, circonstances de recueil, impact du consentement).

Recommandation n° 60

Inscrire dans la loi que les données doivent être traitées d'une manière qui permette à la personne concernée d'exercer effectivement ses droits (principe d'effectivité), en particulier par le biais d'internet lorsque c'est envisageable ;

Conforter l'effectivité du droit à l'information en exigeant que les renseignements fournis à la personne soient accessibles, lisibles et formulés dans un langage compréhensible par le plus grand nombre. À cette fin, encourager la constitution de formats normalisés pour la présentation de ces informations (canevas ou conditions standard d'utilisation des données personnelles par exemple).

Recommandations n° 61 et 62

Afin de renforcer l'effectivité du consentement :

– **n° 61** : prévoir que la personne bénéficie d'une solution de rechange si elle ne souhaite pas que ses données fassent l'objet d'une collecte et d'un traitement ;

– **n° 62** : instaurer un droit au retrait du consentement.

Recommandation n° 63

Consacrer un droit au déréférencement des informations inexactes, incomplètes, équivoques ou périmées apparaissant dans les résultats présentés par les moteurs de recherche.

Recommandation n° 64

Encadrer ce droit au déréférencement afin de concilier de manière adéquate les droits au respect de la vie privée et à la protection des données personnelles, la liberté d'expression et le droit à l'information.

Recommandation n° 65

Instituer un droit à la restitution des données collectées aux individus dont elles émanent, dans des formats ouverts et standards et de manière complète et non dégradée (droit à la portabilité des données).

Recommandation n° 66

Créer de nouveaux droits pour les individus faisant l'objet d'algorithmes qui peuvent avoir une incidence sur leur vie, notamment les algorithmes prédictifs ou à caractère décisionnel, en instaurant un droit d'opposition au profilage et en les soumettant à des exigences d'intervention humaine effective, de transparence et de non-discrimination.

Recommandation n° 67

Instaurer devant la CNIL un droit spécifique d'alerte pour les salariés des entreprises traitant des données personnelles qui souhaitent signaler des pratiques contraires à la législation ou non-conformes aux engagements pris par le responsable du traitement.

Recommandation n° 68

Créer une action collective destinée à faire cesser les manquements à la législation sur les données personnelles, ouverte à certains groupements, associations et syndicats présentant un intérêt à agir.

C. CONFORTER LA PROTECTION DE LA SPHÈRE PRIVÉE À L'HEURE DE LA SURVEILLANCE INSTITUTIONNELLE

Recommandation n° 69

Interdire le recours à des dispositifs algorithmiques de traitements de données transitant par les réseaux numériques aux fins de détection de « signaux faibles » ou de menaces, quelle que soit la finalité poursuivie.

Recommandation n° 70

Encadrer par la loi le recours à l'ensemble des techniques et moyens susceptibles d'être à la disposition des services de renseignement pour remplir leurs missions et mettre un terme aux éventuelles pratiques illégales en sanctionnant plus durement les infractions à la législation.

Recommandation n° 71

Soumettre chaque technique de renseignement à des garanties appropriées et équivalentes, quel que soit leur prétendu degré d'intrusion dans la vie privée.

Recommandation n° 72

Accorder aux citoyens des garanties fondamentales face aux activités de surveillance administrative par la définition précise des conditions et motifs des atteintes susceptibles d'être portées aux droits à la vie privée et à la protection des données personnelles, la réaffirmation de leur proportionnalité et subsidiarité, l'encadrement de la surveillance des communications à l'étranger et l'instauration de voies de recours effectives pour contester certaines pratiques.

Recommandation n° 73

Instaurer un contrôle externe permanent de la mise en œuvre des techniques de renseignement par la création d'une autorité administrative indépendante et impartiale, dotée des moyens humains, matériels, techniques et financiers suffisants.

Recommandation n° 74

Confier à cette autorité des compétences élargies à l'ensemble des services de renseignement et à l'intégralité des mesures qu'ils sont susceptibles de prendre, en lui donnant des prérogatives de contrôle *a priori*, en cours d'opération et *a posteriori* ainsi qu'un pouvoir de recommandation et en lui permettant de saisir un juge en cas de méconnaissance des obligations légales par le pouvoir exécutif.

Recommandation n° 75

Créer un droit de signalement devant l'autorité administrative indépendante chargée de contrôler la mise en œuvre des techniques de renseignement permettant aux agents impliqués dans ces activités de mettre au jour des pratiques illégales.

Recommandation n° 76

Tirer les conséquences juridiques adéquates de l'arrêt de la CJUE *Digital Rights Ireland et Seitlinger* du 8 avril 2014 en limitant la durée de conservation des données techniques de connexion au strict nécessaire ainsi que l'étendue de l'accès accordé à ces données aux autorités publiques.

Recommandation n° 77

Encadrer strictement l'utilisation par les services de police et de justice des techniques spéciales d'investigation susceptibles de porter atteinte aux droits au respect de la vie privée et à la protection des données personnelles :

– les soumettre à l'autorisation préalable d'un magistrat judiciaire indépendant et limitée dans le temps ;

– prévoir des garanties renforcées lorsqu'elles s'appliquent à certaines professions ou fonctions traditionnellement protégées par le code de procédure pénale ;

– les cantonner à la poursuite des infractions délictuelles et criminelles les plus graves.

Recommandation n° 78

Comme en matière de renseignement, écarter la mise en œuvre de programmes conduisant à l'exploitation et au croisement systématiques et à grande échelle des données disponibles sur les réseaux ou recueillies par des technologies de surveillance.

*

* *

IV. DÉFINIR DE NOUVELLES GARANTIES INDISPENSABLES À L'EXERCICE DES LIBERTÉS À L'ÈRE NUMÉRIQUE

A. LE DROIT D'ACCÈS À INTERNET : UN DROIT À CONSACRER

Recommandation n° 79

Reconnaître aux plans national et européen le droit d'accès à internet comme condition d'exercice de plusieurs droits fondamentaux. Préciser que la protection effective de ce droit exige des interventions publiques adéquates pour surmonter toute forme de fracture numérique – culturelle, infrastructurelle, économique – en ce qui concerne l'accessibilité.

Réformer la directive service universel du 7 mars 2002 afin de permettre la mise en place d'une tarification sociale de l'internet.

Recommandation n° 80

Afin de renforcer l'effectivité du droit d'accès à l'internet, instituer un droit pour chacun d'accéder à la « littératie » numérique.

B. LA NEUTRALITÉ DES RÉSEAUX : UN PRINCIPE À CONSACRER

Recommandation n° 81

Consacrer dans la loi ou le règlement de l'Union européenne le principe de neutralité des opérateurs de communications électroniques dans la définition suivante : un traitement égal et sans discrimination, restriction ni interférence de l'ensemble du trafic, quels que soient l'expéditeur ou le destinataire, le contenu consulté ou diffusé, l'application ou le service utilisés ou fournis et les équipements terminaux utilisés.

Recommandation n° 82

Préserver l'accès à un internet ouvert en instaurant une liberté de choix des terminaux et des technologies de réseau par les utilisateurs finals et un contrôle des accords et pratiques commerciales qui régissent le volume de données, le débit et le tarif.

Recommandation n° 83

N'autoriser les mesures de gestion du trafic que si :

– elles sont raisonnables, transparentes, proportionnées, non-discriminatoires et fondées sur des différences objectives entre catégories de trafic équivalentes ;

– elles ne conduisent pas à bloquer, ralentir, modifier, restreindre, perturber, dégrader ou traiter de manière discriminatoire certains contenus, applications ou services, sauf si elles visent à satisfaire une obligation précisément et clairement définie par le législateur (exécution d'une décision de justice, préservation de l'intégrité et de la sûreté du réseau, prévention d'une congestion imminente du réseau ou atténuation des effets d'une congestion temporaire ou exceptionnelle).

Recommandation n° 84

Encadrer strictement le développement des « services spécialisés » :

– l'optimisation de ces services doit répondre objectivement aux caractéristiques spécifiques et essentielles du contenu, de l'application ou du service concerné et nécessiter leur fourniture à un certain niveau de qualité ;

– ils ne doivent pas être fournis au détriment de la disponibilité ou de la qualité générale des services d'accès à l'internet ni être proposés en remplacement de ces derniers ;

– prévoir la notification préalable à l'ARCEP de tout accord conclu entre les fournisseurs de contenus, d'applications et de services et les opérateurs de communications électroniques portant sur ce type de services afin qu'elle puisse s'y opposer en cas de risque de dégradation de la qualité du service général d'accès à l'internet.

Recommandation n° 85

Créer les conditions pour qu'un utilisateur dispose d'un terminal « de confiance » lui permettant d'exécuter toutes les tâches qu'il souhaite et de n'en accomplir aucune sans son consentement. À cette fin, privilégier une approche multiforme : encouragement à la production et à l'usage de « biens communs informationnels » (comme les logiciels libres), soutien des fabricants et éditeurs européens, instauration d'exigences d'interopérabilité et de contrôles des logiciels utilisés par le secteur public, mobilisation des autorités de contrôle en matière de respect de la vie privée, de sécurité des systèmes d'information et de concurrence…

Recommandation n° 86

Renforcer le contrôle de l'ARCEP sur le marché de l'interconnexion.

Recommandation n° 87

Renforcer la transparence sur la qualité des offres d'accès à internet, les risques de congestion des réseaux, les pratiques de gestion de trafic, le marché de l'interconnexion, ce qui suppose d'attribuer à l'ARCEP les moyens nécessaires à l'exercice de ses missions de surveillance et d'observation.

C. LA « LOYAUTÉ DES PLATEFORMES » : UN OBJECTIF À POURSUIVRE PAR L'ADAPTATION DU DROIT COMMUN ET LA MISE EN PLACE D'UNE RÉGULATION SPÉCIFIQUE DES GRANDES PLATEFORMES

Recommandation n° 88

Améliorer l'efficacité du droit de la concurrence face aux problématiques spécifiques de l'économie numérique :

– encourager le recours à des mesures conservatoires destinées à empêcher que des situations n'évoluent de manière irréversible au détriment des partenaires des plateformes ;

– proposer une adaptation des critères d'examen des opérations de concentration et de qualification d'une position dominante afin de mieux appréhender, au-delà du seul chiffre d'affaires, un potentiel de croissance non monétisé assis sur la collecte et le traitement de données à caractère personnel ou l'existence d'une base d'utilisateurs susceptibles de générer de la valeur et des effets de réseau importants ;

– s'écarter d'une approche « en silo » de la régulation concurrentielle pour apporter une réponse globale aux problèmes soulevés par les plateformes, notamment à l'occasion du contrôle des concentrations.

Recommandation n° 89

Agir pour la mise en œuvre d'un dispositif européen interdisant certaines pratiques commerciales restrictives afin de prévenir ou de sanctionner les comportements visant à :

– obtenir d'un partenaire commercial un avantage quelconque ne correspondant à aucun service commercial effectivement rendu ou manifestement disproportionné au regard de la valeur du service rendu ;

– soumettre un partenaire commercial à des obligations créant un déséquilibre significatif dans les droits et obligations des parties ;

– obtenir, sous la menace d'une rupture brutale totale ou partielle des relations commerciales, des conditions manifestement abusives concernant notamment les prix, les délais de paiement, les modalités de vente.

Recommandation n° 90

Adapter les différentes branches du droit commun afin de mieux appréhender les problématiques propres aux plateformes numériques :

– renforcer l'application des obligations de transparence et de loyauté des plateformes à l'égard des consommateurs ;

– poursuivre l'objectif d'encadrement des pratiques des plateformes en matière d'utilisation des données à caractère personnel dans le cadre du projet de règlement européen relatif à la protection des données à caractère personnel ;

– adapter la fiscalité à l'ère numérique et lutter contre l'optimisation fiscale à laquelle se livrent les grandes plateformes en privilégiant une action coordonnée aux niveaux international et européen.

Recommandation n° 91

Pour certains membres de la Commission, il convient de privilégier l'approche par le droit commun et une nouvelle régulation spécifique doit rester une solution de dernier ressort et s'appuyer sur une analyse précise des dysfonctionnements du marché et des gains attendus de la régulation ainsi que de ses effets secondaires sur l'écosystème d'internet.

Pour la majorité des membres de la Commission, l'approche par l'adaptation du droit commun peut être complétée par la mise en place d'une régulation spécifique, portant sur les acteurs dominants de l'économie numérique.

*

* *

V. DESSINER UNE NOUVELLE FRONTIÈRE ENTRE PROPRIÉTÉ ET COMMUNS

Recommandation n° 92

Le développement des communs numériques appelle leur reconnaissance positive dans le droit français, de manière à garantir l'accès à la ressource commune et son partage équitable, contre les éventuelles revendications d'exclusivité.

Recommandation n° 93

La Commission estime qu'il est notamment possible de faire usage de l'article 714 du code civil afin de reconnaître une ressource en tant que commun numérique, en confiant à la puissance publique le rôle de garant de la jouissance commune, si nécessaire par une loi de police.

Recommandation n° 94

La Commission recommande de faire d'internet un commun au niveau mondial. La reconnaissance d'un statut de patrimoine commun de l'humanité pourrait être envisagée, sans exclure d'autres instruments juridiques internationaux. Les organes de gouvernance devront rendre compte de leur gestion commune de cette ressource, notamment au regard du principe de neutralité du réseau.

Recommandation n° 95

La Commission réaffirme la nécessité d'encourager la préservation et l'enrichissement des communs numériques dans le cadre d'une politique volontariste d'open data des données publiques.

Recommandation n° 96

La Commission estime que le domaine public informationnel doit faire l'objet d'une reconnaissance positive en droit français.

Recommandation n° 97

Encourager la pratique des mécanismes volontaires de mise à disposition ouverte des œuvres de l'esprit, notamment à travers des licences libres, en œuvrant à la levée des obstacles qui limitent leur usage.

Recommandation n° 98

Garantir aux auteurs et aux artistes un intéressement juste et équitable aux fruits de l'exploitation numérique de leurs œuvres, en intégrant notamment les économies liées à la production et à la diffusion numériques dans les assiettes et les taux des rémunérations qui leur sont dues.

Recommandations n° 99

Reconnaître à l'auteur un droit à l'exploitation secondaire, afin que la version de l'auteur déposée dans une archive institutionnelle reste en accès libre quelles que soient les suites éditoriales données à ces travaux.

Recommandation n° 100

Rendre librement accessibles les publications scientifiques financées sur fonds publics, après un délai d'exclusivité limité à quelques mois permettant l'activité commerciale de l'éditeur.

Encourager les chercheurs à mettre en accès libre les données brutes et anonymisées de la recherche, à chaque fois que cela ne se heurte pas à des questions déontologiques ou de vie privée.

V. LISTE DES PERSONNALITÉS AUDITIONNÉES

La Commission a procédé aux auditions suivantes dont les comptes rendus sont accessibles sur internet à l'adresse : http://www.assemblee-nationale.fr/14/cr-comnum/14-15/

*Audition de **M. Daniel Kaplan**, délégué général de la Fondation pour l'Internet nouvelle génération, au cours de la réunion du mercredi 25 juin 2014 à 19 heures*

*Table ronde sur le cadre juridique de la liberté d'expression et de communication à l'ère numérique avec les intervenants suivants : **Mme Marie Mongin**, vice-présidente de la 17e chambre du Tribunal de grande instance de Paris et **M. Giuseppe di Martino**, président de l'Association des sites internet communautaires (ASIC), au cours de la réunion du jeudi 3 juillet 2014 à 8 heures 30*

*Audition de **M. Serge Daël**, président de la Commission d'accès aux documents administratifs (CADA), et de **Mme Corinne Bouchoux**, sénatrice et rapporteure de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques, au cours de la réunion du mercredi 9 juillet 2014 à 17 heures*

*Audition de **M. Patrick Eveno**, spécialiste de l'histoire des médias sur le droit à l'information à l'ère numérique et audition de **M. William Bourdon**, avocat, sur la question des lanceurs d'alerte et de l'*habeas corpus *numérique, au cours des réunions du jeudi 25 septembre 2014 à 8 heures 30 et à 9 heures 30*

*Audition de **M Henri Verdier**, directeur d'Étalab, administrateur général des données sur l'*open data *et de **M. Mohammed Adnène Trojette**, conseiller référendaire de la Cour des comptes, sur le principe de gratuité d'usage des données publiques, au cours de la réunion du mercredi 1er octobre 2014 à 18 heures 30*

*Audition de **Mme Maryvonne de Saint–Pulgent**, présidente de la section du rapport et des études du Conseil d'État, de **M. Jacky Richard**, président adjoint, rapporteur général, et de **M. Laurent Cytermann**, rapporteur général adjoint (présentation de l'étude du Conseil d'État sur le « numérique et les droits fondamentaux ») et audition de **M. Olivier Schrameck**, président du Conseil supérieur de l'audiovisuel (CSA), au cours des réunions du jeudi 16 octobre 2014 à 8 heures 30 et à 11 heures*

Table ronde sur les libertés et les activités de renseignement avec ***M. Jean-Marie Delarue****, président de la commission nationale de contrôle des interceptions de sécurité (CNCIS), et* ***M. Jean-Jacques Urvoas****, président de la Commission des lois de l'Assemblée nationale, membre de la CNCIS et audition de* ***M. Jean-Marc Manach****, journaliste, spécialiste des questions de surveillance et de vie privée sur Internet, auteur du blog* Bug Brother*, au cours des réunions du jeudi 13 novembre 2014 à 8 heures 30 et à 10 heures 30*

Audition de ***Mme Isabelle Falque-Pierrotin****, présidente de la Commission nationale de l'informatique et des libertés (CNIL) et audition de* ***M. Marc Robert****, procureur général près la Cour d'appel de Versailles, auteur du rapport « Protéger les internautes » sur la cybercriminalité, au cours des réunions du mercredi 26 novembre 2014 à 17 heures et à 21 heures 30*

Audition de ***M. Jean-Ludovic Silicani****, président de l'Autorité de régulation des communications électroniques et des postes (ARCEP), sur la neutralité des réseaux, au cours de la réunion du jeudi 4 décembre 2014 à 8 heures 30*

Table ronde sur les « données personnelles et les activités économiques » avec ***M. Benoît Tabaka****, directeur des politiques publiques de Google France,* ***M. Paul-Olivier Gibert****, directeur de Digital & Ethics, et* ***M. Pierre Bellanger****, fondateur et président-directeur général du groupe Skyrock le jeudi 18 décembre 2014 à 8 heures 30*

Audition de ***Mme Axelle Lemaire****, secrétaire d'État chargée du numérique, auprès du ministre de l'économie, de l'industrie et du numérique, au cours de la réunion du mercredi 18 mars 2015 à 16 heures 30*

Visioconférence avec les membres de la « Commission numérique » de la ***Chambre des députés italienne****, jeudi 26 mars 2015 à 11 heures*

Audition de ***Mme Christine Lazerges****, présidente de la Commission nationale consultative des droits de l'homme (CNCDH), de* ***M. Pascal Beauvais****, rapporteur, et de* ***M. Hervé Henrion****, conseiller juridique à la CNCDH, sur la liberté d'expression et la lutte contre les contenus illicites sur Internet, au cours de la réunion du mercredi 15 avril 2015 à 18 heures 30*

Audition de ***M. Benoît Thieulin****, président du Conseil national du numérique (CNNum), au cours de la réunion du mercredi 17 juin 2015 à 18 heures 30*

Audition de ***M. Bruno Lasserre****, président de l'Autorité de la concurrence, sur la régulation et la loyauté des plateformes numériques, au cours de la réunion du mardi 7 juillet 2015 à 9 heures 30*

VI. LISTE DES PERSONNES RENCONTRÉES À BRUXELLES (5 MARS 2015)

● **Commission européenne**

M. Andrus Ansip, vice-président chargé du marché unique du numérique,

Direction générale de la justice et des consommateurs :

– **Mme Chiara Adamo**, chef d'unité chargée des droits fondamentaux et des droits de l'enfant

– **M. Bruno Gencarelli**, chef d'unité chargé de la protection des données

Direction générale des réseaux de communication du contenu et des technologies :

– **M. Anthony Whelan**, directeur chargé des réseaux et des services de communication électronique

● **Conseil de l'Union européenne**

Mme Thérèse Blanchet, directrice auprès de la direction justice et affaires intérieures du service juridique du Conseil de l'Union européenne

● **Parlement européen**

M. Jan-Philip Albrecht, rapporteur sur la proposition de règlement du PE et du Conseil 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

Mme Marju Lauristin, rapporteure sur la proposition de directive sur la protection des données dans les domaines judiciaire et policier

● **Représentation permanente de la France auprès de l'UE**

M. Florian Blazy, conseiller juridique

Mme Brigitte Faverel, adjointe au conseiller juridique, chargée des droits d'auteur

Mme Michèle Dubrocard, conseillère justice chargée de la protection des données

M. Pascal Rogard, conseiller chargé des télécommunications et de la société de l'information