Droits et Débats

La France dans la transformation numérique : quelle protection des droits fondamentaux ?

Un colloque organisé
par le Conseil d'État
(section du rapport et des études)
le 6 février 2015

Publications du Conseil d'État chez le même éditeur

Collection « Les rapports du Conseil d'État » (ancienne collection « Études et documents du Conseil d'État », EDCE)

- Le contrat, mode d'action publique et de production de normes (EDCE n° 59), 2008.
- Droit au logement, droit du logement (EDCE n° 60), 2009.
- L'eau et son droit (EDCE n° 61), 2010.
- Consulter autrement, participer effectivement, (EDCE n° 62), 2011.
- Les agences : une nouvelle gestion publique ? – étude annuelle 2012, n° 63.
- Le droit souple – étude annuelle 2013, n° 64.
- Le numérique et les droits fondamentaux – étude annuelle 2014, n° 65.
- L'action économique des personnes publiques – étude annuelle 2015, n° 66.

Collection « Les études du Conseil d'État »

- Le droit de préemption, 2008.
- L'implantation des organisations internationales sur le territoire français, 2008.
- Les recours administratifs préalables obligatoires, 2009.
- La révision des lois bioéthiques, 2009.
- Les établissements publics, 2010.
- Développer la médiation dans le cadre de l'Union européenne, 2011.
- Vers l'institution d'un parquet européen, 2011.
- Le rescrit : sécuriser les initiatives et les projets, 2014.
- L'application du nouveau principe « silence de l'administration vaut acceptation », 2014.
- Les commissaires du Gouvernement dans les entreprises, 2015.
- Directives européennes : anticiper pour mieux transposer, 2015.

Collection « Droits et Débats »

- Le droit européen des droits de l'homme, n° 1, 2011.
- Les développements de la médiation, n° 2, 2012.
- La valorisation économique des propriétés des personnes publiques, n° 3, 2012.
- La démocratie environnementale, n° 4, 2012.
- Consulter autrement, participer effectivement, n° 5, 2012.
- Le patrimoine immatériel des personnes publiques, n° 6, 2013.
- Santé et justice : quelles responsabilités ?, n° 7, 2013.
- Les agences : une nouvelle gestion publique?, n° 8, 2013.
- Les enjeux juridiques de l'environnement, n° 9, 2014.
- La décentralisation des politiques sociales, n° 10, 2014.
- 1952-2012 : le juge français de l'asile, n° 11, 2013.
- Corriger, équilibrer, orienter : une vision renouvelée de la régulation économique – Hommage à Marie-Dominique Hagelsteen, n° 12, 2014.
- La sanction : regards croisés du Conseil d'État et de la Cour de cassation, n° 13, 2015.
- Ou va l'État? – Tome 1, n° 14, 2015.
- Impôt et cotisation : quel financement pour la protection sociale ?, n° 15, 2015.

Collection « Histoire et mémoire »

- Conférences Vincent Wright – volume 1, 2012.
- Conférences Vincent Wright – volume 2, 2015.

Collection « Jurisprudences ».

- Jurisprudence du Conseil d'État 2012-2013, 2014.

Sommaire

Abréviations et acronymes

AMF	Autorité des marchés financiers
ARCEP	Autorité de régulation des communications et des postes
CGU	Conditions générales d'utilisation
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
Convention EDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales
Cour EDH	Cour européenne des droits de l'homme
FNAED	Fichier national automatisé des empreintes digitales
FNAEG	Fichier national automatisé des empreintes génétiques
G29	Groupe de travail Article 29 sur la protection des données (réunion des CNIL européennes)
HADOPI	Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet
LCEN	Loi pour la confiance dans l'économie numérique, n° 2004-575 du 21 juin 2004
NIR	Numéro d'inscription au répertoire
NTIC	Nouvelles technologies de l'information et de la communication
PRISM	Programme américain de surveillance électronique par la collecte de renseignements à partir d'Internet et de certains fournisseurs de services électroniques
TAJ	Traitement d'antécédents judiciaires
TFUE	Traité sur le fonctionnement de l'Union européenne

Avant-propos

Par Jacky Richard,
conseiller d'État,
rapporteur général de l'étude annuelle 2014 du Conseil d'État
« Le numérique et les droits fondamentaux »

Pourquoi organiser un colloque sur le *Numérique et les droits fondamentaux*, cinq mois seulement après la publication de l'étude annuelle du Conseil d'État consacrée au même sujet ? La question est légitime. Un effet de redondance n'était-il pas à craindre, voire une certaine autosatisfaction à redouter ?

Il n'en a rien été, ainsi que l'a montré le déroulement du colloque dont le présent numéro de *Droits et Débats* retrace les échanges. Trois raisons à cela.

Au regard du risque de redite du contenu de l'étude, les organisateurs ont entendu privilégier la dimension européenne et internationale des thématiques retenues, afin de montrer que la France n'est ni seule ni isolée pour affronter la transition numérique. L'animation de la troisième table ronde, intitulée « Le droit des États dans un univers transnational : quelle territorialité ? », par la présidente de la Société de législation comparée, Bénédicte Fauvarque-Cosson, professeur de droit international privé, le confirmerait, si besoin en était.

Au regard du risque de l'autosatisfaction et de la promotion des préconisations du rapport, les organisateurs du colloque ont plutôt pris l'option inverse, celle de mettre en débat les propositions les plus saillantes de l'étude en faisant appel à des intervenants connus pour leur franc parler et leur esprit critique : maître Alain Bensoussan et le député Christian Paul, par exemple. Ainsi le colloque s'est-il emparé, parfois avec passion, des questions suivantes : y a-t-il un droit de propriété des personnes sur leurs données personnelles ? N'est-il pas plus efficace de mettre en avant un droit de la personne, fondé sur le concept d'« autodétermination informationnelle » dont le colloque a approfondi la définition et les contours ? Quelle est la pertinence du concept de « plateforme » en tant que nouvelle catégorie juridique ? Les obligations qui lui seraient attachées sont-elles suffisantes au regard de la protection des données personnelles ou, au contraire, excessives au regard de la liberté d'entreprendre et de l'ouverture à l'innovation ? La préconisation du Conseil d'État consistant à promouvoir le principe du droit du pays de l'internaute, et non celui de l'établissement du site internet en cause, est-elle réaliste ? Quelle est, en la matière, la robustesse du concept de « loi de police », au sens du droit international privé ?

La troisième raison est que le colloque avait également une autre ambition : celle de contribuer à nourrir les nombreuses réflexions actuelles sur le numérique, alors que nombre de réformes sont en cours d'élaboration, tant au niveau national qu'au niveau européen.

Au plan national, le Gouvernement a finalisé un projet de loi sur le numérique après une large concertation de neuf mois confiée au Conseil national du numérique (CNN). L'étude du Conseil d'État fut l'une des bases de cette concertation. Les dispositions centrales du projet de loi *Pour une République numérique* portent sur l'économie de la donnée et du savoir, la valorisation des données massives (*big data*) et la protection des données personnelles, sujets qui se trouvaient au cœur de l'étude du Conseil d'État. Par ailleurs, ce dernier a été auditionné à deux reprises par l'Assemblée nationale pour présenter les conclusions de ses travaux.

Au plan européen, deux règlements sont en cours de discussion entre le Parlement européen et le Conseil, sur la protection des données personnelles et le marché unique des télécommunications. Plusieurs rencontres ont eu lieu entre le Conseil d'État et des responsables d'institutions européennes pour discuter puis présenter les propositions de l'étude, dont bon nombre ont vocation à être traduites dans le droit de l'Union européenne. Les débats du colloque ont, de fait, largement porté sur les évolutions nécessaires de ce droit.

Un tel colloque, tenu dans l'enceinte du Palais royal, ne pouvait pas ne pas être l'occasion de largement revenir sur les deux arrêts que la Cour de justice de l'Union européenne venait de rendre, revêtant l'un et l'autre, pour le sujet débattu, une importance capitale : l'arrêt *Digital Rights Ireland* du 8 avril 2014, qui déclare contraire à la Charte des droits fondamentaux de l'Union une directive de 2006 imposant aux opérateurs de télécommunications la conservation des « métadonnées » de leurs utilisateurs ; l'arrêt *Google Spain* du 13 mai 2014 qui, de son côté, reconnaît l'existence d'un « droit au déréférencement » souvent qualifié de « droit à l'oubli ». Les échanges sur ces deux arrêts, jusque là peu commentés par la doctrine, furent particulièrement éclairants.

L'actualité juridictionnelle est décidément très riche dans ce domaine puisque, postérieurement au colloque, la Cour de justice de l'Union européenne, par une décision du 6 octobre 2015, *Maximillian Schrems vs Data Protection Commissioner*, a invalidé la décision par laquelle la Commission européenne avait établi que les États-Unis, dans le cadre de l'accord dit « *Safe harbour* », assuraient un niveau suffisant de protection des données à caractère personnel européennes. Le colloque, notamment sa troisième table ronde, avait largement débattu de cette question du niveau suffisant de protection des données personnelles transférées aux États-Unis.

Lors de la conclusion du colloque qu'elle a prononcée, dans le cadre d'un exercice original, à deux voix avec Andreas Paulus, juge à la Cour constitutionnelle fédérale d'Allemagne, Maryvonne de Saint Pulgent, présidente de la section du rapport et des études du Conseil d'État, indiquait avec conviction que « *Sur internet, les rapports de droit peuvent sans doute passer par un dialogue des juges, mais j'ai toujours eu tendance à penser que ce sont également des rapports de force* ». Les récentes initiatives de la Commission européenne en matière de localisation des bénéfices fiscaux des grandes plateformes numériques, ainsi que la réaction des autorités américaines qui a suivi, confortent cette conviction.

Puissent les actes de ce colloque apporter à tous ceux qui s'intéressent à ces sujets majeurs les éléments d'une réflexion juridique et politique approfondie.

Programme du colloque

9h00 - 9h15 – Séance d'ouverture

Jean-Marc Sauvé, vice-président du Conseil d'État

9h15 - 11h00 – Table ronde n° 1 : Quelle protection des données personnelles pour quelle conception de la vie privée ?

Président : **Jacky Richard**, conseiller d'État, président adjoint et rapporteur général de la section du rapport et des études du Conseil d'État

Intervenants : **Alain Bensoussan**, avocat à la Cour d'appel de Paris

Antonio Casilli, sociologue, maître de conférences à Télécom ParisTech, chercheur au Centre Edgar Morin (EHESS)

Thomas von Danwitz, président de chambre à la Cour de justice de l'Union européenne

Délia Rahal-Löfskog, chef du service de la santé à la CNIL

11h00 - 12h45 – Table ronde n° 2 : Quelle régulation des plateformes numériques ?

Président : **Christian Paul**, député de la Nièvre, coprésident de la commission de réflexion sur le droit et les libertés à l'âge du numérique

Intervenants : **Nicolas Colin**, inspecteur des finances, entrepreneur

Laurent Cytermann, maître des requêtes au Conseil d'État

Francis Donnat, directeur des relations institutionnelles et des politiques publiques de Google France

Antoinette Rouvroy, chercheuse qualifiée au centre de recherche « information, droit et société », faculté de droit de Namur

14h00 - 15h45 – Table ronde n°3 : Le droit des États dans un univers transnational : quelle territorialité ?

Président : **Bénédicte Fauvarque-Cosson**, professeur de droit à l'université Panthéon-Assas, présidente de la Société de législation comparée

Intervenants : **Édouard Geffray**, secrétaire général de la CNIL

Winston Maxwell, avocat associé à Hogan Lovells

Marc Mossé, directeur des affaires juridiques et publiques, membre du comité de direction de Microsoft France

Alain Strowel, professeur à l'université Saint-Louis (Bruxelles) et à l'université catholique de Louvain

15h45 - 16h30 – Séance de clôture du colloque

Maryvonne de Saint Pulgent, présidente de la section du rapport et des études du Conseil d'État

Andreas Paulus, juge à la Cour constitutionnelle fédérale d'Allemagne

Avertissement – les fonctions des intervenants sont celles exercées à la date du colloque.

Séance d'ouverture

Jean-Marc Sauvé
vice-président du Conseil d'État

Diplômé de Sciences Po Paris et ancien élève de l'École nationale d'administration, Jean-Marc Sauvé entre comme auditeur au Conseil d'État en 1977. Il est conseiller technique dans les cabinets de Maurice Faure et de Robert Badinter, ministres de la justice, de 1981 à 1983. Il occupe les postes de directeur de l'administration générale et de l'équipement au ministère de la justice de 1983 à 1988, puis de directeur des libertés publiques et des affaires juridiques au ministère de l'intérieur de 1988 à 1994, date à laquelle il devient préfet de l'Aisne. Nommé maître des requêtes au Conseil d'État en 1983, il devient conseiller d'État et secrétaire général du Gouvernement en 1995. Depuis le 3 octobre 2006, il est le vice-président du Conseil d'État. Il est également président du comité prévu par l'article 255 du Traité pour le fonctionnement de l'Union européenne (comité de sélection des juges européens), président du conseil d'administration de l'ENA et président de l'Institut français des sciences administratives. En juin 2012, il a été élu pour deux ans président de l'Association des Conseils d'État et des juridictions administratives suprêmes de l'Union européenne.

« *Avec la révolution numérique, c'est un nouvel imaginaire qui domine nos sociétés. L'objet fétiche, sur le modèle duquel le monde est conçu, n'est plus l'horloge et son jeu de forces mécaniques, mais l'ordinateur et sa puissance de calcul. (…) La révolution numérique va ainsi de pair avec celle qui s'observe en matière juridique, où l'idéal d'une gouvernance par les nombres tend à supplanter celui du gouvernement par les lois. (…) Se pose, ainsi, la question de la domestication par les hommes des nouvelles techniques immatérielles, qui peuvent aussi bien contribuer à libérer qu'à écraser leurs capacités de création* »[1]. Cette question, que soulève le professeur Alain Supiot, s'adresse à l'État, régulateur des relations sociales et des flux économiques, mais aussi garant des droits fondamentaux des personnes et de l'ordre public. Elle s'adresse à la France, comme nation souveraine, mais aussi comme État membre de l'Union européenne et, dès lors, partie prenante à l'élaboration de sa législation. Elle s'adresse aussi à l'Union européenne dans son ensemble, car la transformation numérique déborde le cadre des États-nations, elle innerve des marchés d'ampleur mondiale et elle ne supprime bien sûr ni les rivalités économiques, ni les rapports de force géopolitiques, ni la capacité de régulation des États, qu'elle affaiblit cependant. La transformation numérique est une transformation technique et elle appelle désormais une transformation juridique qui doit être conduite, conformément au principe de subsidiarité, à l'échelle nationale et européenne.

1 A. Supiot, « Grandeur et misère de l'État social », leçon inaugurale au Collège de France, prononcée le 29 novembre 2012, p. 23.

Cette transformation, comme l'a montré l'étude annuelle du Conseil d'État en 2014[2], doit porter en priorité sur le cœur de notre État de droit et de notre souveraineté, à savoir sur la protection des droits fondamentaux et sur la sécurité et la sûreté publiques. Les technologies numériques exercent, à ce titre, des effets ambivalents : elles catalysent l'exercice des droits, mais elles synthétisent aussi des risques *inédits* face auxquels nos catégories juridiques et nos capacités d'intervention apparaissent aujourd'hui inadaptées. La protection de la vie privée et la faculté d'autodétermination des personnes doivent être mieux protégées, les responsabilités des opérateurs économiques, entre hébergeurs, plateformes et éditeurs, doivent être redistribuées et les capacités de régulation, de contrôle et d'intervention des États doivent être sécurisées. Nous ne pouvons pas nous abstenir d'agir, en nous retranchant derrière la technicité des débats sur le numérique, encore moins derrière la prétendue impuissance des États face à ce nouvel aspect de la globalisation. Car il importe que, par le droit et, en dernière instance, sous le contrôle des juges, soient mis en balance des intérêts parfois concurrents, ceux des opérateurs, des internautes et des citoyens et, au-delà d'eux, des intérêts publics essentiels et des intérêts privés.

C'est précisément à cette tâche que le présent colloque nous invite. Je présenterai, tout d'abord, les domaines dans lesquels une adaptation de notre droit est attendue, avant d'insister sur le cadre territorial de mise en œuvre de nouveaux outils.

I. Face à la transformation numérique, mieux protéger les droits fondamentaux, c'est renforcer les capacités d'autodétermination des personnes, mais c'est aussi redistribuer les responsabilités entre les différents acteurs numériques.

A. En premier lieu, si le principe de consentement encadre d'ores et déjà le traitement des données à caractère personnel, une réflexion doit être engagée sur les modalités pratiques de sa mise en œuvre.

Deux phénomènes ont, en effet, rebattu les cartes. D'une part, l'automatisation du traitement des données à caractère personnel relativise et, en fait, minimise l'exigence de consentement éclairé, lequel est d'autant plus formel ou entravé que les conditions d'utilisation de ces données sont présentées d'une manière inintelligible ou subreptice. À ce titre, comme l'a jugé le Conseil d'État, l'effectivité du droit d'accès aux données – et du droit de rectification – doit être appréciée à l'aune de la complexité de leurs procédures concrètes de mise en œuvre[3]. D'autre part, la massification des données (en anglais, « *big data* »[4]) et le développement corrélatif des techniques d'agrégation et de profilage affaiblissent les principes garantissant la qualité des données. Ces dernières, comme le prévoit l'article 6 de la directive du 24 octobre 1995[5], doivent être traitées d'une manière loyale, être

2 Étude du Conseil d'État, *Le numérique et les droits fondamentaux*, la documentation Française, 2014.

3 CE, 12 mars 2014, *Société Pages jaunes groupe*, req. n° 353193.

4 Mégadonnées ou données massives (en anglais, « *big data* ») sont des « *données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés* » (J.O. du 22 août 2014).

5 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

collectées pour des finalités déterminées, de manière proportionnée et pour une durée limitée, mais aussi être exactes, complètes et mises à jour. Or de la qualité des données traitées, dépend aussi l'effectivité du principe de consentement, désormais protégé par l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

C'est pourquoi il apparaît nécessaire de réaffirmer ce principe et de réexaminer ses modalités pratiques de mise en œuvre. L'étude du Conseil d'État préconise à cette fin d'inscrire dans notre droit positif le principe *d'autodétermination informationnelle*[6], plutôt qu'un droit de propriété sur les données à caractère personnel. En effet, un tel droit ne saurait rééquilibrer à lui seul les relations entre les personnes et les opérateurs numériques, dans la mesure où les données d'un seul individu n'ont, sauf exception, qu'une faible valeur marchande. Par ailleurs, en introduisant une logique mercantile, ce droit de propriété réduirait la portée des garde-fous mis en place par les autorités publiques. « *Somme toute, la reconnaissance du droit de propriété impliquerait une moindre capacité de protection des pouvoirs publics, sans renforcer pour autant la capacité des individus à veiller à leurs propres intérêts* »[7].

Le droit d'autodétermination informationnelle apparaît ainsi plus approprié à la défense du principe de consentement. Tel que défini par la Cour constitutionnelle fédérale allemande, ce droit garantit en effet « *la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* »[8], dans l'intérêt de son épanouissement, mais aussi dans l'intérêt global d'une société libre et démocratique. Un tel droit inaliénable peut, dès lors, servir de point d'appui à l'élaboration de nouvelles protections contre tout risque d'abus ou d'utilisation illicite des données personnelles par des personnes privées ou publiques. À ce titre, si la prévention des infractions les plus graves appelle un renforcement des capacités de contrôle et de surveillance des autorités publiques, les impératifs de sécurité et de sûreté nationales doivent être conciliés d'une manière exigeante avec la protection des libertés individuelles. Il ne suffit pas, en effet, qu'un traitement se prévale d'une finalité légitime, il doit encore user, d'une manière claire et précise, de moyens adéquats et proportionnés au but visé. C'est ce qu'a rappelé avec force la Cour de justice de l'Union européenne en invalidant, par son arrêt *Digital Rights*[9], la directive du 15 mars 2006 sur la conservation des données traitées dans le cadre de services de communications électroniques accessibles au public[10]. Moins qu'une prohibition générale et absolue des obligations de conservation des données à caractère personnel, il faut désormais mettre en œuvre des critères clairs et objectifs de collecte et surtout d'accès à ces données.

---

libre circulation de ces données.

6 V. Annexe 3.

7 Étude du Conseil d'État, *Le numérique et les droits fondamentaux*, la Documentation française, 2014, p. 267.

8 BVerfGE 65, 1 – Volkszählung, 15 décembre 1983.

9 CJUE, Gde Ch., aff. C-293/12, 8 avril 2014, *Digital Rights Ireland Ltd*.

10 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.

B. En second lieu, les responsabilités doivent être mieux distribuées entre les différents acteurs numériques en tenant compte des nouvelles techniques de mise à disposition des données.

Si les éditeurs de site sont soumis à un régime de responsabilité analogue à celui des éditeurs de presse, les hébergeurs voient, quant à eux, leur responsabilité civile et pénale limitée, dès lors qu'ils ne jouent qu'un rôle passif d'intermédiation et qu'ils n'ont pas connaissance des données qu'ils stockent. Cette s*umma divisio* entre hébergeurs et éditeurs apparaît désormais en partie obsolète, car des entités revendiquant le statut d'hébergeur, parmi lesquelles des sites de partage ou des moteurs de recherche, opèrent en réalité un traitement actif et profond sur les données personnelles, qu'elles les indexent, les référencent ou les classent. Plusieurs décisions de justice, nationale et européenne, témoignent de l'inadéquation entre la qualification d'hébergeur, son régime de responsabilité et la réalité de pratiques observées[11]. Dès lors qu'il détermine lui-même les finalités et les moyens d'un traitement, l'hébergeur doit être en mesure d'assumer les obligations incombant à un « *responsable de traitement* », au sens de la directive 95/46. C'est ce qu'a jugé la Cour de justice de l'Union européenne dans son arrêt *Google Spain* : « *en explorant de manière automatisée, constante et systématique Internet à la recherche des informations qui y sont publiées* », l'exploitant du moteur de recherche procède à un traitement dont il définit les finalités et les moyens. Or, « *dans la mesure où l'activité d'un moteur de recherche est susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites web les droits fondamentaux de la vie privée (…), l'exploitant de ce moteur de recherche (…) doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que [son activité] satisfait aux exigences (…) d'une protection efficace et complète des personnes concernées* »[12]. La Cour a abouti à cette conclusion à partir d'une analyse très concrète des pratiques de référencement et de leurs effets sur la vie privée des personnes[13].

Dans ce cadre, l'étude annuelle du Conseil d'État propose de créer un régime autonome de responsabilité pour les prestataires actifs de services d'intermédiation, autrement appelés « *plateformes* ». Celles-ci seraient tenues de respecter un principe de loyauté dans la mise en œuvre de leurs services de référencement ou de classement et, à ce titre, de faire connaître la pertinence de leurs critères éditoriaux, de notifier les évolutions de leur politique commerciale et, enfin, de mettre en place un *droit au déréférencement* – à distinguer d'un « droit à l'oubli » –

11 V. en ce qui concerne un site de place de marché : CJUE, Gde Ch., aff. C-324/09, 12 juillet 2011, *L'Oréal c. eBay* ; Cour de Cassation, com., 3 mai 2012, *eBay c. Société Parfums Christian Dior*, n°11-10.508 ; en ce qui concerne un moteur de recherche : CJUE, Gde Ch., aff. C-236/08, 23 mars 2010, *Google France Inc. c. Louis Vuitton Malletier*.

12 CJUE, Gde Ch., aff. C-131/12, 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, paragr. 38.

13 « *l'organisation et l'agrégation des informations publiées sur Internet effectuées par les moteurs de recherche dans le but de faciliter à leurs utilisateurs l'accès à celles-ci peut conduire, lorsque la recherche de ces derniers est effectuée à partir du nom d'une personne physique, à ce que ceux-ci obtiennent par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet leur permettant d'établir un profil plus ou moins détaillé de la personne concernée* », CJUE, Gde Ch., 13 mai 2014, *Google Spain* précité, paragr. 37.

qui consisterait en l'effacement du contenu des données. Les obligations positives de transparence et de contrôle qui en découlent ne sauraient, cependant, porter atteinte à la nature même de leur activité : le principe de neutralité, appliqué aux opérateurs de télécommunication, ne peut régir utilement leurs services qui ont précisément pour objet de fournir un accès hiérarchisé et personnalisé aux contenus numériques. La liberté éditoriale des plateformes est un acquis à préserver mais, comme toute liberté, elle s'accompagne de responsabilités et de devoirs qu'il faut désormais identifier et rendre opposables[14].

II. Pour mener à bien cette adaptation de notre droit, une réflexion doit être menée sur son champ d'application territorial, dans un environnement marqué par la concurrence, sinon la rivalité, entre systèmes juridiques.

A. La transformation numérique emprunte les réseaux ramifiés de la globalisation, elle est transfrontalière dans ses effets et ses acteurs se singularisent par leur forte extranéité. La complexité des règles qui déterminent la loi applicable et la juridiction compétente peut être source d'incertitudes, d'insécurité juridique et de remise en cause des protections nationales.

1. Le droit pénal s'est, en premier lieu, ajusté face aux nouvelles menaces dont peuvent être le vecteur les technologies numériques. Il trouve, en effet, à s'appliquer aux sites, même établis hors de nos frontières, qui dirigent leurs activités vers la France au regard d'une pluralité d'indices (langue et monnaie utilisées, terminaison du nom de domaine, publicités visibles par les internautes français, etc.)[15]. Cette territorialité directionnelle a conduit les juges français à faire usage de leurs pouvoirs d'injonction à l'encontre de sociétés étrangères. Il a, par exemple, été enjoint, dans l'affaire *LICRA et UEJF c. Yahoo!,* à la société *Yahoo* de rendre inaccessible un site vendant des objets de propagande nazie[16], ou encore, dans l'affaire *Max Mosley c. Google*, à la société *Google* de faire cesser l'affichage d'images attentatoires à la vie privée[17]. Dans la première affaire, les demandes présentées par la société *Yahoo* tendant à ce que les décisions de la justice française ne soient pas exécutables aux États-Unis ont été rejetées à deux reprises par une juridiction d'appel américaine[18]. Cette dernière a pu relever que « *la France était en droit en tant que nation souveraine d'adopter des lois contre la distribution de propagande nazie, en réponse à sa terrible expérience des forces nazies durant la seconde guerre mondiale* » et que « *Yahoo! ne pouvait s'attendre à bénéficier du fait que ses contenus puissent être vus dans le monde entier, tout en étant protégée des coûts qui en résultent* »[19].

---

14 À cet égard, la société *Google* a mis en place un comité consultatif qui vient de publier son rapport sur les conditions de mise en œuvre du droit au déréférencement : https:// www.google.com/intl/fr/advisorycouncil/

15 Cour de Cassation, crim., 9 septembre 2008, *Giuliano*, n° 07-87.281.

16 Ordonnance du 22 mai 2000 du juge des référés du tribunal de grande instance de Paris.

17 TGI de Paris 6 novembre 2013, *Max Mosley c. Google Inc. et Google France*, RG 11/07970.

18 Cour d'appel fédérale du 9ème circuit, 23 août 2004 et 12 janvier 2006, *LICRA and UEJF v. Yahoo!*, n° 01-17424.

19 Étude du Conseil d'État, *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 138.

Toutefois, la prévention et la répression des infractions pénales ne peuvent être pleinement efficaces que par une coopération renforcée entre autorités judiciaires, mais aussi, en amont, entre les autorités administratives et les sociétés de l'Internet. À cet égard, les opérateurs et les hébergeurs sont tenus de conserver pendant un an les métadonnées[20] de leurs utilisateurs et de les transmettre, à sa demande, à l'autorité judiciaire[21]. Les autorités administratives peuvent aussi obtenir la communication de ces données dans le cadre de leurs missions de protection de la sécurité nationale[22]. Or, les grandes sociétés de l'Internet ayant la qualité d'hébergeur ne s'estiment pas tenues par ces obligations et répondent, à leur guise et selon leurs propres critères, aux demandes qui leur sont adressées. Sans vouloir la stigmatiser, la société *Facebook,* dont les centres de données (en anglais, « *Datacenters* ») se situent aux États-Unis, à l'exception d'un site en Suède à Luleå, n'a ainsi répondu entre juillet et décembre 2013 qu'à 33,9 % de ces demandes. Il faut dire que la loi du 21 juin 2004[23] ne détermine pas elle-même le champ d'application des obligations de coopération des hébergeurs et que le décret du 25 février 2011, pris pour son application, ne renvoie qu'au territoire national[24] ou, comme cela a pu être interprété, au champ d'application de la loi du 6 janvier 1978[25].

2. En second lieu, dans le domaine des obligations contractuelles, le droit applicable est, par principe, librement déterminé par les parties[26] et, à défaut, un contrat ayant pour objet une prestation de service est régi par la loi du pays de résidence habituelle du prestataire[27]. Toutefois, s'agissant des contrats conclus par un consommateur avec un professionnel, le droit applicable est la loi du pays où le consommateur a sa résidence habituelle, si le professionnel exerce son activité dans ce pays ou s'il y dirige son activité par tout moyen[28]. Pour autant, même dans ce cas, les parties restent libres de déterminer une autre règle de territorialité, à condition, toutefois, qu'elle n'ait pas pour effet de priver le consommateur des protections indérogeables prévues par la loi de son pays de résidence[29]. Par ailleurs, en cas de litige, le consommateur peut se prévaloir de règles spécifiques, dès lors que son cocontractant exerce ses activités dans l'État de l'Union où le

20 Définies à l'art. 1 du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

21 Art. 6, II, de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

22 Art. L. 246-1 du code de la sécurité intérieure, créé par la 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.

23 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (dite « LCEN »).

24 À l'exception des Terres australes et antarctiques françaises, voir art. 12 du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

25 Voir ordonnance du juge des référés du tribunal de grande instance de Paris, 24 janvier 2013, *UEJF et autres c. Twitter Inc. et Twitter France*.

26 Art. 3 du règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (dit « Rome I »).

27 Art. 4, §1, b), du règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (dit « Rome I »).

28 Art. 6, § 1, du règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (dit « Rome I »).

29 Art. 6, § 2, du règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (dit Rome I).

consommateur a élu domicile ou dirige ses activités vers cet État[30]. Parmi ces règles, lorsque l'action est intentée contre le consommateur par son cocontractant, seules sont compétentes les juridictions de l'État de l'Union sur le territoire duquel est domicilié ce consommateur [31]. Néanmoins, comme l'a souligné l'étude du Conseil d'État[32], les pratiques commerciales observées tendent à faire prévaloir le droit du professionnel et, le plus souvent, la compétence de juridictions étrangères. C'est, notamment, le cas des conditions générales d'utilisation (CGU) proposées par les grandes firmes américaines.

B. Dans ces conditions, une réflexion doit être engagée sur une refonte du champ d'application des protections essentielles et sur les conditions de leur effectivité.

Un socle de règles choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public devrait être déterminé et rendu applicable dans les pays de destination de l'activité considérée. Comme le préconise le Conseil d'État[33], serait ainsi étendue, au-delà du champ pénal, la règle selon laquelle les sites dirigeant leurs activités, par exemple vers la France, sont soumis aux règles de cet État. Dans le domaine contractuel, ces règles regardées comme essentielles et dont le champ d'application devrait ainsi être refondu pourraient être qualifiées de « *lois de police* » au sens du règlement européen du 17 juin 2008, dit Rome I. Ces lois comportent en effet des dispositions impératives « *dont le respect est jugé crucial par un pays pour la sauvegarde de ses intérêts publics, tels que son organisation politique, sociale ou économique, au point d'en exiger l'application à toute situation entrant dans son champ d'application, quelle que soit par ailleurs la loi applicable au contrat* »[34]. S'agissant des obligations de coopération imposées aux hébergeurs, une même adaptation de notre droit devrait être envisagée.

Ce changement de paradigme ne saurait être présenté, d'une manière offensive, comme la promotion d'une extraterritorialité conquérante du droit national ou européen. Il s'agit, bien plutôt, de préserver, d'une manière claire et non contingente, les garanties essentielles adoptées par certains États au bénéfice de leurs résidents. C'est vers ce nouveau progrès de l'État de droit que s'est engagée l'Union européenne. Dans l'affaire *Google Spain* du 13 mai 2014, le traitement des données litigieuses était, en effet, réalisé par la société-mère établie aux États-Unis, et non pas par sa filiale européenne établie en Espagne. Pour autant, la Cour a relevé que « *les activités de l'exploitant du moteur de recherche et celles de son établissement situé dans l'État membre concerné sont indissociablement liées, dès*

30 Art. 17, 1, c), du règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (refonte). La Cour de justice de l'Union utilise alors un faisceau d'indices pour déterminer si le professionnel « dirige » ses activités vers l'État de domiciliation du consommateur ; voir CJUE, Gde Ch., aff. C-585/08, 7 décembre 2010, *Pammer et Hôtel Alpenhof*.

31 Art. 18, 1, du règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (refonte).

32 Étude du Conseil d'État, *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 140.

33 *Ibid*, p. 243.

34 Art. 9 du règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (dit Rome I).

lors que les activités relatives aux espaces publicitaires constituent le moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités »[35]. Dans ces conditions, la Cour a conclu qu'« *il ne saurait être accepté que le traitement de données à caractère personnel effectué pour les besoins du fonctionnement dudit moteur de recherche soit soustrait aux obligations et aux garanties prévues par la directive 95/46, ce qui porterait atteinte à l'effet utile de celle-ci et à la protection efficace et complète des libertés et des droits fondamentaux des personnes physiques qu'elle vise à assurer* »[36]. Avec cet arrêt, s'est considérablement affaibli le lien entre le lieu de traitement des données à caractère personnel et l'application des garanties européennes. Cette nouvelle approche converge avec la refonte en cours d'examen des règles européennes relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. La proposition de nouveau règlement européen prévoit, en effet, de s'appliquer « *au traitement des données à caractère personnel appartenant à des personnes concernées ayant leur résidence sur le territoire l'Union, par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées (…) à l'offre de biens ou de services à ces personnes concernées dans l'Union ou (…) à l'observation de leur comportement* » [37].

Vous le voyez, les défis qu'adresse à notre droit la transformation numérique nous invitent à une révolution de nos catégories et paradigmes juridiques. Alors qu'un projet de loi national sur le numérique et une proposition de règlement européen sont à l'étude, cette adaptation doit être menée d'une manière homogène et ambitieuse en Europe, mais aussi d'une manière coopérative avec nos partenaires extra-européens. Son objectif reste cependant clair : il s'agit de mettre davantage les technologies numériques au service des droits fondamentaux des résidents européens. C'est à partir de ce point d'ancrage personnel que doit se déployer le *droit du numérique* qui est désormais une composante essentielle des droits de l'Homme.

35 CJUE, Gde Ch., aff. C-131/12, 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, paragr. 56 ; la Cour précise, en outre, que « *[L'] affichage des résultats [du traitement des données à caractère personnel] étant accompagné, sur la même page, de celui de publicités liées aux termes de recherche, force est de constater que le traitement de données à caractère personnel en question est effectué dans le cadre de l'activité publicitaire et commerciale de l'établissement du responsable du traitement sur le territoire d'un État membre, en l'occurrence le territoire espagnol*. », paragr. 57.

36 CJUE, Gde Ch., aff. C-131/12, 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, paragr. 58.

37 Art. 3, 2, de 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 (règlement général sur la protection des données), COM(2012) 11 final.

Première table ronde

Quelle protection des données personnelles pour quelle conception de la vie privée?

La table ronde a pour ambition d'aborder la question sensible du statut des données personnelles. Existe-t-il un droit de propriété des personnes sur leurs données personnelles ? Ne convient-il pas d'envisager la protection des données personnelles autrement que comme un droit patrimonial, c'est-à-dire plutôt comme un droit de la personne à l'autodétermination informationnelle ? Des exemples concrets tirés de l'utilisation des données de santé et de l'usage du numérique dans les relations de travail, de l'exposition de la vie privée sur les réseaux sociaux permettraient de vérifier la pertinence du choix de la meilleure protection des données personnelles.

Sommaire





Éléments de réflexion sur la protection des données personnelles

Un droit de propriété des personnes sur leurs données contre un principe affirmant la primauté de la personne ?

Face aux limites actuelles de la protection des données à caractère personnel, il est parfois proposé de donner aux individus un véritable droit de propriété sur leurs données. Le but recherché est notamment de susciter une implication plus active : les individus devenant financièrement intéressés à une bonne gestion de leurs données.

Le Conseil d'État ne recommande pas d'emprunter cette voie en dépit de son attrait apparent. S'il convient en effet de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant ce droit comme un droit à l'autodétermination plutôt que comme un droit de propriété.

En l'état du droit, il n'existe pas de droit de propriété de l'individu sur ses données personnelles, mais un dispositif juridique de droits attachés à la personne. Il convient d'écarter l'introduction d'une logique patrimoniale dans la protection des données personnelles car il n'est certainement pas souhaitable que l'individu, par l'exercice du droit d'aliénation attaché au droit de propriété, renonce à toute protection de ses données personnelles.

C'est dans cette mesure que le Conseil d'État envisage le droit à la protection des données personnelles comme un droit à l'autodétermination informationnelle, plutôt que comme un droit de propriété, c'est-à-dire « le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel » (proposition 1 de l'étude annuelle 2014).

Le Conseil d'État propose ce concept d'*autodétermination informationnelle*, dans une logique proche de celle consacrée par la Cour constitutionnelle fédérale de l'Allemagne. Celle-ci, dans un arrêt du 15 décembre 1983 relatif à une loi sur le recensement, a établi sur le fondement des articles 1er (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale allemande, que « *la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* ». 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. Il ne s'agit plus seulement de protéger le droit au respect de la vie privée mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté.

Dans cette perspective, la notion d'autodétermination informationnelle servirait à fonder non pas un droit supplémentaire, comme le droit d'information, le droit d'accès, le droit de rectification mais un principe essentiel car donnant sens à d'autres droits fondamentaux, qui tendent alors à le garantir.

Afin de doter cette notion d'une portée étendue à l'ensemble des États membres, le Conseil d'État propose que ce principe de l'autodétermination informationnelle soit inscrit dans les considérants de la proposition de règlement européen relatif à la protection des données, ou par anticipation, dans la loi française relative à l'informatique, aux fichiers et aux libertés de 1978.

Quelle position de l'Europe sur la protection des données personnelles ? Quelle marge de manœuvre de la France pour faire évoluer le droit de l'Union ?

Le droit européen des données personnelles repose sur une pluralité de textes (Charte des droits fondamentaux de l'Union européenne, directive de l'Union européenne du 24 octobre 1995, convention n° 108 du Conseil de l'Europe du 28 janvier 1981) qui définissent plusieurs grands principes : collecte des données loyale, répondant à des finalités déterminées et proportionnée à ces finalités ; exigence du consentement de la personne ou d'un autre principe prévu par la loi ; droits d'information, d'accès, de rectification et d'opposition de la personne ; existence d'une autorité indépendante de contrôle.

L'ensemble constitue un *corpus* juridique cohérent et protecteur qui diffère de manière substantielle du droit américain, dans lequel il n'existe pas de cadre général du traitement des données personnelles et qui retient une approche subjective, centrée sur la réparation du préjudice subi. En revanche, d'autres espaces juridiques sont plus proches du droit européen : des pays tels que le Brésil ou la Corée du sud ont adopté au cours de ces dernières années une législation protectrice.

La proposition de règlement relative à la protection des données personnelles, soumise en 2012 au Conseil et au Parlement européen, a pour but de substituer un régime harmonisé de protection des données aux différentes lois nationales transposant la directive de 1995. La nature de la règle juridique concernant la protection des données serait ainsi modifiée : elle ne serait plus nationale mais européenne. Ce renforcement de l'intégration juridique (passage du niveau de la directive à celui du règlement) apparaît nécessaire compte tenu du caractère transnational du fonctionnement d'Internet et de la dimension des grandes entreprises du numérique.

Dès lors, l'échelon européen revêt aujourd'hui un caractère central. Nombre des propositions de l'étude du Conseil d'État relèvent de la compétence de l'Union européenne, soit parce qu'elles impliquent une modification du droit de l'Union, soit parce que l'Union européenne constitue, en opportunité, le niveau pertinent d'action. La France peut, compte tenu de son poids au sein du Conseil, contribuer de manière importante à l'action européenne.

Toutefois, il est apparu au Conseil d'État qu'un nombre, certes limité, de propositions pouvaient être portées en priorité par les autorités nationales car les délais de mise au point des directives ou des règlements peuvent être longs. Par conséquent, il apparaît opportun aux autorités françaises d'être force de propositions en la matière, par exemple pour ce qui concerne les sujets suivants : protection des données personnelles, garanties en faveur des organes de presse ou réglementation de la responsabilité des plateformes numériques. D'autres sujets touchent aux intérêts fondamentaux de notre pays : il en est ainsi des modalités de conservation des données de communication à des fins de prévention ou de répression.

Conciliation entre la protection de la vie privée et les impératifs de la sécurité publique et de la sûreté nationale.

Le numérique a renforcé les moyens d'action de la police et des services de renseignement. Les fichiers de police ont grandement bénéficié de l'essor du numérique. Les services de renseignement ont, quant à eux, de plus en plus recours à la surveillance des communications électroniques. L'affaire PRISM de 2013 a fait de la question un élément clé du débat public. Le Conseil d'État préconise de mieux assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques, tout en conciliant cet objectif avec les impératifs de la sécurité publique et de la sûreté nationale.

Si l'usage de fichiers par la police est ancien, le numérique a changé la nature de leur utilisation par les facilités de recherche et de conservation qu'il procure. En 2013, le fichier Traitement d'antécédents judiciaires (TAJ) comptait ainsi plus de douze millions de fiches . La conservation des empreintes et l'usage des données biométriques ont également bénéficié du développement numérique : en témoignent l'essor du Fichier national automatisé des empreintes digitales (FNAED) ou génétiques (FNAEG). Face à cette situation, le Conseil d'État juge souhaitable de renforcer les garanties entourant l'utilisation de ces fichiers. Sans remettre en cause leur utilité pour les services de police, il propose de mieux tirer les conséquences des décisions judiciaires (classement sans suite, non-lieu, relaxe et acquittement) et de définir concernant le TAJ un plan d'apurement des erreurs (propositions n° 34 et 35).

Pour ce qui concerne la prévention des atteintes à la sécurité et à la sûreté nationale, il convient de la concilier avec le respect des droits fondamentaux. La collecte de renseignement par la surveillance des communications électroniques est un élément essentiel de la stratégie de défense et de sécurité de la France. Les deux livres blancs de 2008 et de 2013 en ont fait une priorité, en prévoyant une augmentation des moyens alloués aux services de renseignement afin de mieux faire face aux nouvelles menaces, notamment liées au terrorisme.

Les principes encadrant la surveillance des communications par les pouvoirs publics en France ont été fixés par la loi du 10 juillet 1991 . Toutefois, l'essor du numérique a, depuis, démultiplié les capacités d'interception et d'analyse des données. Au niveau européen, le cadre juridique de la conservation des données de communication a été remis en cause par la CJUE dans son arrêt *Digital Rights Ireland* qui invalide la directive du 15 mars 2006 relative à la conservation des données par les opérateurs de télécommunication, en estimant que l'atteinte à la vie privée commise lors de leur interception et de leur stockage ne doit pas être disproportionnée par rapport aux objectifs poursuivis par les pouvoirs publics.

Compte tenu des termes de l'arrêt Digital Rights Ireland, deux interprétations sont possibles : l'une, stricte, condamnant par principe tout système de conservation générale des métadonnées ; l'autre, plus ouverte, permettant le maintien d'un tel système mais avec des garanties plus fortes que celles prévues par la directive du 15 mars 2006. Le Conseil d'État considère que la remise en cause, par principe, de la conservation générale des métadonnées poserait d'importantes difficultés pour

l'efficacité du renseignement et de la police judiciaire. La portée de l'arrêt Digital Rights Ireland pourrait être précisée par la CJUE à l'occasion d'un nouveau renvoi préjudiciel d'une juridiction nationale devant elle.

Le Conseil d'État propose de prendre, dès à présent, les mesures qu'impose l'arrêt *Digital Rights Ireland*, même dans son interprétation ouverte. Il préconise notamment de réserver l'accès aux métadonnées à des fins de police judiciaire aux crimes et délits d'une gravité suffisante, et de réexaminer les régimes prévoyant l'accès de diverses autorités administratives (par exemple : la HADOPI, l'AMF ou l'administration fiscale) à des fins autres que la sécurité intérieure.

Il propose aussi d'étendre aux procédures d'accès aux métadonnées les garanties prévues en faveur des parlementaires, avocats, magistrats et journalistes pour les interceptions judiciaires (proposition 38).

Le Conseil d'État propose par ailleurs de définir par la loi le régime de l'interception des communications à l'étranger, en fixant leurs finalités et en prévoyant leur contrôle par une autorité administrative indépendante (proposition 39).

Opportunité de la mise en place d'un numéro d'identification unique non signifiant et d'un élargissement du domaine d'utilisation du Numéro d'inscription au répertoire (NIR) au secteur de la santé et de la recherche médicale.

La mise en place d'un numéro d'identification unique non signifiant en complément ou en substitut au Numéro d'inscription au répertoire (NIR) utilisé pour les traitements de données relatifs à la sécurité sociale permettrait de lever certaines appréhensions concernant le respect de la vie privée. En effet, le NIR est un numéro signifiant qui fournit des informations sur le sexe, l'année, le mois ainsi que le lieu de naissance. Le Conseil d'État préconise de mettre à l'étude la création de ce numéro national non signifiant et d'évaluer son intérêt pour la conduite des politiques publiques et la simplification des démarches administratives. Le numéro national non signifiant serait généré de manière aléatoire (proposition 21).

Le Conseil d'État propose, à plus courte échéance, de faciliter l'utilisation du NIR au secteur de la santé et de la recherche médicale afin de favoriser les politiques publiques de recherche et de prévention. Or, actuellement, l'utilisation du NIR est fortement encadrée par la loi car c'est un numéro d'identification signifiant. Cet encadrement est susceptible de constituer un obstacle à des traitements d'utilité publique ne présentant pas de risques pour la vie privée. L'étude annuelle préconise ainsi de supprimer l'obligation de passer par un décret en Conseil d'État pour autoriser les traitements effectués à des fins de recherche dans le domaine de la santé ; seul l'avis rendu par la CNIL en vertu du chapitre IX de la loi du 6 janvier 1978 serait nécessaire pour mener à bien l'utilisation du NIR pour les traitements de données à des fins de recherche médicale (proposition 22).

Cette proposition du Conseil d'État va dans le même sens que le changement de doctrine d'utilisation du NIR annoncé par la CNIL dans son rapport d'activité pour 2013. La CNIL admet désormais que le NIR soit utilisé comme identifiant national pour les données de santé alors qu'elle avait jusqu'ici toujours affirmé la nécessité d'un « cantonnement » au domaine de la sécurité sociale.

Présentation des intervenants

Modérateur

Jacky Richard, *conseiller d'État, rapporteur général, président adjoint de la section du rapport et des études du Conseil d'État*

Ancien élève de l'École normale supérieure (Saint-Cloud) et de l'École nationale d'administration, agrégé de géographie, Jacky Richard a fait une grande partie de sa carrière au ministère de l'Éducation nationale où il fut chef de bureau à la direction des affaires financières, secrétaire général de l'académie de Toulouse, directeur de l'administration générale et des personnels, et chef du corps de l'inspection générale de l'administration de l'éducation nationale et de la recherche (IGAENR). De mai 2001 à septembre 2005 il fut directeur général de l'administration de la fonction publique (DGAFP) et, parallèlement, jusqu'en février 2003, délégué interministériel à la réforme de l'État. En 2005, il est nommé conseiller d'État et affecté à la section du contentieux puis, parallèlement, membre de la section de l'administration. Depuis mai 2010, il est rapporteur général et président adjoint de la section du rapport et des études (SRE) du Conseil d'État. Par ailleurs, il a présidé de 2007 à 2014 le conseil d'administration du Centre national de gestion des praticiens hospitaliers et des directeurs d'hôpital. Depuis 2010, il préside le conseil d'administration de l'École nationale supérieure de la police (ENSP). Il préside également le comité de déontologie du Conseil général de l'alimentation, de l'agriculture et des espaces ruraux.

Intervenants

Alain Bensoussan, *avocat à la Cour d'appel de Paris*

Dès 1978, Alain Bensoussan, avocat à la Cour d'appel de Paris, spécialiste en droit de l'informatique, en droit de la propriété intellectuelle et en droit international, a fondé un cabinet dédié au droit des technologies avancées. Il participe à de nombreux groupes de réflexion dans ce domaine et est à l'origine de concepts comme les droits de l'homme numérique, ou encore le droit des robots. Une biographie plus détaillée peut être consultée sur le site Wikipédia à l'adresse suivante : https://fr.wikipedia.org/wiki/Alain_Bensoussan_(avocat)

Antonio Casilli, *sociologue, maître de conférences à Télécom ParisTech, chercheur au Centre Edgar Morin (EHESS)*

Antonio Casilli est maître de conférences en Digital Humanities à Telecom ParisTech et chercheur en sociologie au Centre Edgar Morin (École des hautes études en sciences sociales). Ses recherches portent principalement sur la politique, la santé et les usages informatiques. Depuis 2009, il coordonne plusieurs projets de recherche sur les réseaux sociaux en ligne, la santé et la vie privée. Il s'occupe

aussi de méthodologies avancées de la recherche en sciences sociales, notamment de simulations multi-agents. En plus de plusieurs publications scientifiques en français, anglais et italien, il est le co-auteur de Qu'est-ce que le digital labor ? (ed. INA, 2015) et de Against the Hypothesis of the End of Privacy (ed. Springer, 2014). Ses ouvrages précédents incluent Les liaisons numériques (ed. Seuil, 2010), une étude sur la façon dont l'Internet reconfigure les formes de la sociabilité contemporaine, et Stop Mobbing (ed. DeriveApprodi, 2000), une analyse de la violence communicationnelle dans le capitalisme cognitif. Il a coordonné un numéro spécial de la revue Communications consacré aux cultures du numérique (Seuil, mai 2011). Dans la revue Esprit, il a dirigé le dossier « Le corps à l'épreuve du numérique » (avril 2009).

Thomas von Danwitz, *président de chambre à la Cour de justice de l'Union européenne*

Titulaire d'un examen d'État en droit (1986 et 1992), d'un doctorat en droit (université de Bonn, 1988) et d'un diplôme international d'administration publique (ENA, 1990), Thomas von Danwitz a été nommé professeur de droit public allemand et de droit européen en 1996 à la faculté de droit de l'université de la Ruhr, Bochum, dont il a été le doyen de 2000 à 2001. À partir de 2003, il a enseigné à l'université de Cologne, où il a pris en 2006 la direction de l'institut de droit public et de science administrative. Il a également été professeur invité à la Fletcher School of Law and Diplomacy (2000), à l'université Panthéon-Sorbonne (2005-2006) et à l'université François Rabelais (Tours, 2001-2006), qui lui décerne le titre de docteur honoris causa en 2010. Juge à la Cour de justice de l'Union européenne depuis le 7 octobre 2006, il préside la 8e chambre du 7 octobre 2008 au 6 octobre 2009. Depuis le 11 octobre 2012, il est le président de la 5e chambre.

Délia Rahal-Löfskog, *chef du service de la santé à la Commission nationale de l'informatique et des libertés (CNIL)*

Titulaire de DESS en droit de la bioéthique (université de Paris 12) et en droit de la santé (université de Paris Sud), d'un DEA de l'École des hautes études en sciences sociales ainsi que du certificat d'aptitude à la profession d'avocat (EFB), Délia Rahal-Löfskog a débuté sa carrière en 2003 comme juriste à l'Office national d'indemnisation des accidents médicaux (ONIAM). En 2009, elle a intégré la CNIL, où elle occupe actuellement les fonctions de chef du service de la santé à la direction de la conformité. Elle est par ailleurs auteur de plusieurs publications notamment en droit de la santé.

Actes – Quelle protection des données personnelles pour quelle conception de la vie privée ?

Jacky Richard
Président adjoint et rapporteur général de la section du rapport et des études

Le colloque a pour but de remettre en lumière l'étude annuelle 2014 du Conseil d'État *Le numérique et les droits fondamentaux*. Il a l'ambition, six mois après la publication de cette étude, de mettre en débat un certain nombre des cinquante propositions qui méritent d'être confrontées aux opinions contraires, aux perspectives nouvelles ou différentes qui ont pu apparaître. C'est ce que nous vous proposons de faire ensemble aujourd'hui.

Ainsi, au moment où s'achève la consultation conduite par le Conseil national du numérique sur les enjeux du futur projet de loi sur le numérique que souhaite le président de la République et que porte Mme Axelle Lemaire, ce colloque est-il particulièrement bienvenu. Le Conseil d'État a rassemblé beaucoup de matériaux dans son étude de 2014. Je pense qu'il est utile de débattre des nombreuses pistes qu'il a tracées. Les trois tables rondes qui vont scander notre journée de travail vont nous permettre de le faire.

La première table ronde, que j'ai l'honneur d'animer, portera sur les données numériques et plus précisément sur *les données à caractère personnel*, ce « carburant » du numérique. Nous nous interrogerons pour savoir quelles sont les protections qu'il convient d'y apporter et quelles sont les utilisations, les limites, voire les dangers et/ou les potentialités de ces données à caractère personnel.

La seconde table ronde portera sur le sujet : « *les plateformes numériques, quelles régulations ?* ». Elle sera présidée par le député Christian Paul, qui préside une importante réflexion mixte à l'Assemblée nationale au sein d'une commission spéciale composée à la fois de parlementaires et de personnalités qualifiées et qui porte sur le devenir des protections du numérique. Cette seconde table ronde s'efforcera de déterminer qui sont ces prestataires de services souvent regroupés sous le terme générique et étrange de « plateforme » et qui nous sont à la fois familiers et relativement inconnus.

La troisième table ronde présidée par Mme Bénédicte Fauvarque-Cosson, Professeur d'université, spécialiste de droit international privé et de droit comparé, sera consacrée à *la territorialité d'Internet et au droit des États dans un univers transnational*.

Enfin, en couronnement de cette journée de réflexion, la séquence de clôture du colloque sera une synthèse à deux voix, effectuée par M. Andreas Paulus, juge à la Cour constitutionnelle fédérale d'Allemagne, et Mme Maryvonne de Saint Pulgent, présidente de la section du rapport et des études du Conseil d'État.

Je saisis cette occasion pour dire aux participants que la section du rapport et des études a été, à la fois, le maître d'ouvrage conceptuel de ce colloque et le maître d'œuvre organisationnel. Je souhaite remercier toutes celles et tous ceux qui ont permis qu'il ait lieu, notamment Mme Marie Delord. Enfin, qu'il me soit permis ici de saluer l'exceptionnel travail du rapporteur général adjoint, M. Laurent Cytermann, maître des requêtes, sans qui l'étude annuelle 2014 ne serait pas ce qu'elle est.

Il est temps maintenant de vous présenter les participants de cette première table ronde sur les données à caractère personnel. Tout d'abord, Thomas von Danwitz qui est président de chambre à la Cour de justice de l'Union européenne, professeur de droit public allemand et de droit public européen, doyen de l'université de la Ruhr-Bochum, et directeur et enseignant à l'institut de droit public de Cologne. Il est juge à la Cour de justice de l'Union Européenne depuis 2006. Il a d'abord présidé, à partir de 2008, la 8e chambre, et il préside actuellement la 5e chambre qui a eu à connaître de la décision *Digital rights*[38] dont nous reparlerons.

À ma gauche, Maître Alain Bensoussan, avocat à la Cour d'appel de Paris, spécialiste du droit de l'informatique, du droit de la propriété intellectuelle, du droit international, et très au fait de ces questions du numérique. Il a fondé, depuis des années déjà, un cabinet spécialisé en droit des technologies avancées. Il est président fondateur du premier réseau international des avocats spécialisés dans le droit du numérique ; il enseigne à l'École centrale de Paris ; il est le chroniqueur de nombreuses revues, et il a publié de nombreux articles et de nombreux ouvrages sur le numérique dont la notoriété n'a d'égale que leur originalité.

À sa gauche, Mme Délia Rahal-Löfskog est chef de service santé à la Commission nationale de l'informatique et des libertés. Mme Délia Rahal-Löfskog est diplômée en droit de la bioéthique, en droit de la santé, diplômée de l'École des Hautes études en sciences sociales et a été remarquée pour ses travaux sur la personne dans le droit. Elle a débuté sa carrière comme juriste à l'Office national d'indemnisation des accidents médicaux et elle est actuellement chef de service santé à la CNIL.

Enfin, M. Antonio Casilli est chercheur, sociologue, maître de conférence à Telecom ParisTech, et chercheur à l'École des Hautes études en sciences sociales au centre Edgar Morin. Il est l'auteur de très nombreux articles et ouvrages remarqués ; il coordonne plusieurs recherches sur les réseaux sociaux en ligne, la santé, le travail et la vie privée.

Notre table ronde va se dérouler en deux temps. Nous écouterons tout d'abord Maître Alain Bensoussan et Thomas von Danwitz. Cette première séquence sera consacrée à *la conception de la donnée à caractère personnel* dans le monde du numérique. Il ne s'agit pas là d'un débat théorique ou philosophique, mais d'un débat juridique qui renvoie à des enjeux très concrets sur la protection des données, sur leur utilisation et sur leur mode de production. Les deux autres intervenants pourront intervenir à la suite de leurs propos.

38 CJUE, aff. C-293/12 et C-594/12, 8 avril 2014, *Digital Rights Ireland et Michael Seitlinger*.

La deuxième séquence de cette table ronde sera peut-être moins conceptuelle et plus illustrative. Elle traitera des *conséquences pratiques de la numérisation des données personnelles*. Il s'agira, au travers d'exemples concrets, de comprendre leur signification et leur traitement dans le domaine de la santé. Mme Délia Rahal-Löfskog nous en parlera d'abord, puis, ensuite, M. Antonio Casilli exposera des exemples tirés des différentes facettes de la vie privée et montrera comment les frontières entre vie publique et vie privée, entre travail et loisirs, sont aujourd'hui totalement brouillées.

Pour commencer, je me tourne vers Maître Alain Bensoussan pour qu'il nous présente sa conception de la donnée numérique personnelle fondée sur la propriété de la donnée, sa patrimonialité. Il le sait, nous en avons beaucoup débattu ; ce n'est pas la conception retenue par le Conseil d'État dans son étude. C'est une raison supplémentaire pour lui demander de présenter cette conception. Puis, Thomas von Danwitz apportera la contradiction en traitant de la question de l'autodétermination informationnelle. Il nous expliquera ce que recouvre cette appellation quelque peu sibylline.

Alain Bensoussan
Avocat à la Cour d'appel de Paris

L'étude annuelle 2014 du Conseil d'État est une contribution majeure à la réflexion et à l'action dans le domaine des libertés du numérique, tout particulièrement s'agissant du thème de cette table ronde : la protection des données personnelles. Je ne vous propose pas une plaidoirie, ni une conférence, mais une conversation pour essayer de mettre en place une réflexion pour le futur. Car cette étude n'est sans doute qu'une étape dans ce domaine.

En remarque liminaire, je souhaiterais préciser qu'à l'expression « *droits de l'homme numériques* » je préfère celle de *droits humains virtuels*. En effet, je pense que l'ensemble des acteurs du numérique doit repenser les droits humains, car l'évolution des nouvelles technologies de l'information et de la communication (NTIC) ne fait que commencer. L'Internet est pour moi le jurassique du monde virtuel. Ce constat effectué, il me semble que la loi française dite « *informatique, fichiers et libertés* »[39] ou même la loi fédérale allemande votée en 1976[40], sont restées pertinentes quelles que soient les technologies utilisées (ordinateurs centraux, mini ou micro-ordinateurs, réseaux locaux ou Internet, etc.). J'ai longtemps lutté pour promouvoir la loi française, notamment à travers le droit à l'oubli[41], avant même

39 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (JORF, 7 janvier 1978, p. 227) modifiée 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 (JORF, 7 août 2004, p. 14063) et par la loi n° 2014-344 du 17 mars 2014 relative à la consommation.

40 La loi fédérale allemande de protection des données (en allemand « *Bundesdatenschutzgesetz* ») a été la première adoptée au niveau fédéral en la matière en Allemagne. Votée en 1976 par le *Bundestag*, puis par le *Bundesrat* avant d'être promulguée le 27 janvier 1977, elle est entrée en vigueur le 1er janvier 1978. Elle a ensuite été modifiée à plusieurs reprises. La dernière modification date du 25 février 2015 et entrera en vigueur en janvier 2016.

41 V. contribution d'A. Bensoussan au *Livre blanc des droits de l'homme numérique*, à l'initiative de M. Santini, 20/11/2000, disponible sur : http://www.alain-bensoussan.com/documents/P7ETUDE1.pdf

que la Cour de justice de l'Union européenne ne consacre ce droit. Il me semble cependant aujourd'hui que ce texte a vieilli. Le monde numérique actuel et celui de demain ne peuvent plus se satisfaire d'une extension de la loi « *informatique, fichiers et libertés* ». Le moteur de la technologie devrait être celui du droit ; or, c'est l'inverse qui se produit : le droit est piloté par la technologie. Les lois sur la signature électronique et sur le commerce électronique sont très proches en Allemagne, en France, à Singapour, aux États-Unis, en Chine ou au Japon. Aussi, lorsque les technologies gouvernent le droit, indépendamment de l'approche romano-germanique ou anglo-saxonne, cela n'est pas sans conséquences sur l'évolution du monde numérique et, demain, du monde virtuel.

La donnée est patrimoniale parce que la possession est une valeur universelle. La plupart d'entre nous, quel que soit le pays où il vit, se dit : « *ce sont mes données, mes informations ; c'est mon monde numérique* ». Or lorsque ce droit universel s'exprime avant que les droits légaux ne soient reconnus, il y a matière à s'intéresser à un cadre juridique nouveau. Aussi évoquerais-je, dans un premier temps, le déficit du cadre légal de la protection des données personnelles (1), dans un second temps, la monétarisation de ces données (2) et, enfin, la propriété des données (3).

1. Le *déficit de protection*.

La situation juridique est un *patchwork* composé d'un ensemble de droits de la personnalité dont on peut constater, au-delà de la réflexion juridique, l'échec démocratique. Dans la loi française dite « *informatique, fichiers et libertés* », pionnière en matière de droits du numérique, on a accordé à l'ensemble des individus des droit fondamentaux : droit de questionnement, droit d'accès, droit de modification, droit d'orientation, droit de compréhension des algorithmes. Or, si vous faites un test, et je le fais chaque année auprès des étudiants de l'École centrale de Paris, pour demander par exemple qui a fait usage de son droit d'accès, l'immense majorité répond par la négative. Ainsi, lorsque l'on met en regard l'article premier de cette loi qui précise que « *l'informatique est au service de chaque citoyen* » et la réalité, on s'aperçoit que le citoyen ne met jamais en œuvre ses droits. Certes, c'est une bonne chose que d'avoir des droits numériques sans que l'on ait besoin de se battre constamment pour eux. Mais lorsque l'on a des droits aussi fondamentaux depuis trente-cinq ans qui ne sont pas mis en œuvre par le citoyen, il faut s'interroger sur leur pertinence, non pas théorique ou juridique, mais économique.

Les droits de la personne, le droit à l'image ou à la vie privée, ou encore les droits sur les événements, sont une faillite en termes opérationnels. Alors que le droit à la souveraineté, le droit à l'autodétermination, le droit à la dignité du numérique sont des droits nécessaires. Il n'est cependant pas question pour moi de défendre l'idée que ces droits antérieurs doivent être abandonnés, mais il faut les penser à l'aune de l'Histoire. Ils sont et demeurent fondamentaux.

2. La *monétarisation des données*.

La situation économique aujourd'hui est celle d'une monétarisation rampante[42] parce qu'il existe un déficit du droit de mise en œuvre du droit à la protection des données. Le système de droit virtuel tel qu'il existe est opérationnel, mais il s'agit d'une égalité asymétrique. Pourquoi *Facebook* et *Twitter* ont-ils plus d'un milliard d'inscrits ? Pourquoi les réseaux sociaux sont-ils devenus des valeurs si fortes dans la mise en œuvre de notre personnalité ? Pourquoi dans cette *terre des hommes numériques*, pour s'inspirer du titre d'un ouvrage de Saint-Exupéry[43], toutes ces personnes, quelles que soient leurs cultures, leurs opinions politiques, leurs langues, leurs situations géographiques, se retrouvent-elles sur *Facebook* ou *Twitter* ?

Loin de moi l'idée, par de tels propos, de m'opposer aux conclusions de l'excellente étude annuelle 2014 du Conseil d'État sur *Le numérique et les droits fondamentaux* qui, n'en doutons pas, fera date dans l'action en faveur des droits de l'homme numérique. Il s'agit plus, pour l'avocat que je suis, de se demander si le fait que les réseaux sociaux soient au cœur du monde moderne ne serait pas dû au fait que *Facebook* n'est pas autre chose que *le droit de paraître* ; et que *Twitter* n'est pas autre chose que *le droit universel de parler pour ne rien dire*. Et dans cette égalité asymétrique, le citoyen s'y retrouve. Certes, ce faisant, il donne l'ensemble de ses données à une entreprise qui se les approprie, mais cette dernière se les approprie parce que dans cette égalité asymétrique les acteurs sont dans la logique du don comme toujours dans la pré-économie, au sens de Marcel Mauss et de Maurice Godelier : les gens donnent leurs informations en échange de services, base de l'expression de ce droit universel à exister et à parler[44].

La Charte des droits fondamentaux[45] place dans son article premier la dignité, puis dans son article 8 la protection des données personnelles. L'article 16 du Traité sur le fonctionnement de l'Union Européenne (TFUE) inscrit ces données dans le cadre du droit de l'Union Européenne avec, en sacre, des autorités indépendantes participant à la protection des consommateurs. Il me semble toutefois que cette démarche est insuffisante.

Dans cette optique, un cadre juridique est nécessaire, mais il doit concilier l'ordre public. Ce cadre est essentiel comme le montrent notamment les affaires de piratage massif contre la firme *Sony Pictures* et de vol des données personnelles des clients de la société *Orange*. Le vol est la soustraction frauduleuse de la chose d'autrui ; cette question se retrouve au cœur de la réflexion pénale française mais aussi américaine. Or, actuellement, les rédacteurs de ce droit sont les réseaux sociaux eux-mêmes. *Facebook* écrit dans son contrat de licence que les internautes lui accordent une licence non exclusive. Si cette dernière reconnaît aux internautes un droit de propriété sur leurs données, il n'existe nulle part dans le monde une entité juridique qui reconnaisse un tel droit de propriété. Pourtant

42 V. A. Bensoussan, « Faut-il réguler la marchandisation des données personnelles sur internet ? », du 30 janvier 2013, rubrique « blog expert Droit des technologies avancées » sur le site du *Figaro*, disponible sur http://blog.lefigaro.fr/bensoussan/2013/01/le-profilage-commercial-est-inherent.html

43 A. de Saint-Exupéry, *Terre des hommes*, février 1939.

44 M. Mauss, *Essai sur le don*, PUF, 1968, 4e éd. (paru initialement en 1923-1924 dans l'*Année sociologique*) et Maurice Godelier, *L'énigme du don*, Fayard, 1996.

45 *Charte des droits fondamentaux de l'Union européenne* (2000/C 364/01).

Facebook n'est pas seulement une entreprise américaine ou plutôt mondiale, c'est une société universelle qui accueille plus d'un milliard de personnes à travers un cadre contractuel aux termes duquel les internautes qui font appel à ses services restent propriétaires de leurs données, mais accordent une licence d'utilisation au réseau social. La plupart des autres firmes (*Google*, *Viadeo*, etc.), ont recours à des dispositions plus ou moins similaires pour créer, de façon asymétrique, de la confiance avec les internautes.

3. La *propriété des données*.

En France, selon l'article 2 de la Déclaration des droits de l'homme et du citoyen[46], la propriété est un élément fondamental. L'article 544 du Code civil[47] reconnaît le principe de propriété des choses (comme celui de vol). L'attribution aux personnes d'un droit de propriété sur leurs données personnelles n'a rien d'anodin au plan économique. Elle permet la valorisation en bourse des sociétés comme *Facebook* ou *Google* même si elle n'est que la traduction des possibilités de mieux connaître les individus à travers leurs données personnelles. Il est donc nécessaire de réguler ce nouveau marché pour éviter tout abus.

Dans cette optique, il apparaît souhaitable de mettre en place un cadre juridique conforme à l'ordre public, tenant compte du fait que l'intérêt de l'économie du virtuel est qu'elle génère, – hors vol –, un droit d'appropriation des données sans dépossession des propriétaires. Il y a cependant une difficulté. Nous sommes dans le partage d'informations qui, une fois partagées, ne sont pas perdues pour le propriétaire. À aucun moment il n'y a transfert de propriété avec aliénation d'un bien. Nous devons donc, dans cette conjugaison entre le droit et le numérique, faire preuve d'une créativité nouvelle pour répondre aux enjeux d'une propriété acquise sans dépossession du propriétaire originel. Il faudrait intégrer le concept de *dignité numérique de la personne humaine* qui, malheureusement, n'existe dans aucune loi en tant que telle ; même si la Charte des droits fondamentaux de l'Union européenne le retient dans son article 1er avant même les notions de liberté et de sûreté (article 6) ou de protection des données personnelles (article 8) [48].

Mais la dignité numérique recouvre des acceptions différentes[49]. Les éléments qui la composent doivent prendre en compte ces aspects virtuels, par exemple le droit de chacun d'entre nous non pas à la vie privée, vieux concept géographique, mais à *l'intimité numérique*, y compris au sein du domicile. Aujourd'hui, les données s'achètent et se vendent dans le monde entier. Cela ne me paraît pas contraire au respect de la dignité humaine, regardé comme une composante de l'ordre public, tel qu'il avait été invoqué par exemple dans une décision célèbre condamnant le lancer de nains[50].

46 « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression* », art. 2, DDHC.

47 « *La propriété est le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements* », art. 544 du code civil.

48 « *La dignité humaine est inviolable. Elle doit être respectée et protégée* », art. 1er, Charte des droits fondamentaux de l'Union européenne.

49 V. A. Bensoussan, « Les droits de l'homme numérique », 21 juillet 2010, répertoire « blog expert Droit des technologies avancées » sur le *blog* du *Figaro*, http://blog.lefigaro.fr/bensoussan/2010/07/les-droits-de-lhomme-numerique.html

50 CE Ass., 27 octobre 1995, *Commune de Morsang-sur-Orge*, n° 136727, Rec. Lebon p. 372.

On gardera à l'esprit que le droit est par essence *infra* moral et *supra* économique, mais aussi que le marché est, en économie, l'expression de la démocratie et qu'enfin le droit à l'autodétermination n'est que l'antichambre du droit de propriété.

Jacky Richard

Président adjoint et rapporteur général de la section du rapport et des études

Merci beaucoup pour ce plaidoyer sur la conception patrimoniale de la donnée. Je note dans vos propos les expressions suivantes : « *licence non exclusive ; clause de confiance, certes asymétrique, mais confiance quand même* ». Je pense que dans ces mots-là, se noue une opposition qui n'est pas factice mais qui peut être dépassée.

Thomas von Danwitz

Président de chambre à la Cour de justice de l'Union Européenne

« *L'homme est né libre, et partout il est dans les fers* ». C'est par cette formule célèbre mais assurément dramatique que Jean-Jacques Rousseau introduit ses pensées sur la nécessité d'un contrat social[51], seul à même de garantir la liberté civique des citoyens. Cette phrase a été décrite non sans raison comme le coup de clairon des Lumières[52]. La discussion actuelle sur la protection de la vie privée, dans le cadre de la conservation des données à caractère personnel[53] et les critiques sur le contrôle de ces données opéré notamment par Google[54] a donné lieu à des formules tout aussi dramatiques. Divers groupes politiques et sociaux exigent la mise en place d'un contrat social pour l'ère digitale[55] où l'exploration de la sphère privée par les États et par des grandes entreprises est perçue comme une menace[56]. Ainsi, une déclaration des droits de l'Homme numérique a été récemment publiée en France[57]. Marqués par les attentats récents, les élèves de l'ENA ont baptisé la promotion 2015/2016 « George Orwell » puisqu'ils avaient à cœur de réaffirmer leur attachement à la liberté d'expression et, de manière plus générale, aux libertés qu'il appartient avant tout aux pouvoirs publics de protéger. Au-delà de ces accentuations, il semble que le débat public auquel nous assistons en ce moment s'efforce de trouver des repères et de déterminer nos valeurs. Dès lors, avons-nous besoin d'un nouveau coup de clairon pour répondre aux défis que pose la numérisation pour la protection de la vie privée ?

51 J.-J. Rousseau, *Du contrat social ou Principes du droit politique*, 1762, Livre I, Chapitre 1.

52 I. Fetscher, *Rousseaus politische Philosophie. Zur Geschichte des demokratischen Freiheitsbegriffs,* 1975, S. 102.

53 CJUE, aff. C−293/12 et C−594/12, 8 avril 2014, *Digital Rights Ireland Ltd*, EU:C:2014:238.

54 V. notamment Mathias Döpfner, Offener Brief an Eric Schmidt, *Frankfurter Allgemeine Zeitung* vom 15 avril 2014, p. 9 ainsi que Jaron Lanier, Wer die Daten hat, bestimmt unser Schicksal, *Frankfurter Allgemeine Zeitung* vom 24 avril 2014, p. 9.

55 V. le titre du 2e congrès de Bündnis 90/Die Grünen le 20 octobre 2012, https:// www.gruene-bundestag.de/fraktion/netzpolitischer-kongress (consulté le 27 novembre 2014).

56 H. Welzer, Wenn man etwas merkt, ist es zu spät, *Frankfurter Allgemeine Zeitung* vom 23 avril 2014, S. 9.

57 *Frankfurter Allgemeine Zeitung* Nr. 225 du 27 septembre 2014, p. 9. Cette déclaration du Forum d'Avignon est accessible sur le site www.ddhn.org.

I. L'arrêt *Digital Rights et Seitlinger*

Les réactions[58] concernant l'arrêt de la Cour dans l'affaire *Digital Rights et Seitlinger*[59] ont principalement porté sur la question de savoir si, à la suite de cet arrêt, une rétention des données était en tant que telle exclue ou si elle restait encore possible dans des conditions strictes[60]. Vu le nombre et l'importance des atteintes constatées par la Cour, l'empressement à vouloir minimiser la problématique des droits fondamentaux ne semble, à tout le moins, pas aller de soi, et cela d'autant plus après que les cours constitutionnelles autrichienne[61], slovène[62] et roumaine[63] ont annulé leur législation respective transposant la directive 2006/24[64]. En Slovaquie, la Cour constitutionnelle a privé d'effets juridiques les dispositions transposant la directive portant sur la conservation des données[65], la procédure est encore en cours, et en Suède les fournisseurs de services de communications électroniques ont, à la suite de cet arrêt, cessé de sauvegarder des données[66]. En revanche, l'arrêt de la Cour a été mal accueilli en Grande-Bretagne où une nouvelle législation portant sur la conservation des données a entre temps été adoptée mais expire cependant en 2016[67].

Dans le cadre des discussions portant sur les conséquences à tirer de cet arrêt, il importe qu'une législation nationale, quelle qu'elle soit, portant sur la conservation

58 T. Ojanen, « Privacy is more than just a seven-letter word : the court of justice of the European Union sets constitutional limits on mass surveillance », *European constitutional law review*, 2014, 10(3), 528-541 ; S. Peyrou, « La Cour de justice, garante du droit «constitutionnel» à la protection des données à caractère personnel (CJUE, aff. jointes C-293/12 et C-594/12, 8 avril 2014, *Digital Rights Ireland Ltd*) », *RTD Eur. 2015*, v. 51, n° 1, janvier-mars, p. 117-131 ; C. D. Classen, Datenschutz ja - aber wie ? : Anmerkung zum Urteil des EuGH vom 8.4.2014, verb. Rs. C-293/12 und C-594/12 (*Digital Rights Ireland u.a.*), Europarecht 2014, v. 49, n. 4, p. 441-447 ; A. Rosas et É. Goebel, « Le contrôle par la CJUE des actes de l'Union relatifs au traitement des données au regard de la Charte des Droits », *Revues des Juristes de Sciences Po* n° 10, mars 2015, 115 ; D. Simon, « La révolution numérique du juge de l'Union : les premiers pas de la cybercitoyenneté », *Europe* n° 7, juillet 2014, étude 6.

59 CJUE, aff. jointes C−293/12 et C−594/12, 8 avril 2014, *Digital Rights Ireland e.a.*, EU:C:2014:238.

60 V. J. von Altenbockum, Wir brauchen einen Vorratsdatenschutz, *Frankfurter Allgemeine Zeitung* vom 10 avril 2014, www.faz.net/aktuell/politik/harte-bretter/vorratsdatenspeicherung-wir-brauchen-einen-vorratsdatenschutz-12890139.html (consulté le 27 novembre 2014) ; J. von Altenbockum, Der Justizminister kuscht, *Frankfurter Allgemeine Zeitung* vom 8 avril 2014, http://www.faz.net/aktuell/politik/inland/eugh-zur-vorratsdatenspeicherung-justizminister-heiko-maas-rudert-zurueck-12885567.html (consulté le 27 novembre 2014).

61 Cour constitutionnelle autrichienne, arrêt du 27 juin 2014, G 47/2012, JBl 9/2014, 578 ; communiqué de presse disponible à l'adresse : www.vfgh.gv.at (consulté le 27 novembre 2014). V. Johannes Stoll, VfGH bringt Vorratsdatenspeicherung endgültig zu Fall, SWK, n° 23-24/2014, p. 1068 et suiv.

62 S. Bardutzky, *The Timing of Dialogue : Slovenian Constitutional Court and the Data Retention Directive*, 10 septembre 2014, www.verfassungsblog.de/en/timing-dialogue-slovenian-constitutional-court-data-retention-directive/.

63 Cour constitutionnelle roumaine, Décision n° 440 du 8 juillet 2014, consultable sur le site de la Cour constitutionnelle roumaine: www.ccr.ro/files/products/Decizie_440_2014_reviz.pdf.

64 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 (JO L 105, p. 54).

65 Cour constitutionnelle de la République de Slovaquie, arrêt du 23 avril 2014 – PL ÚS 10/2014.

66 V. l'adresse : www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-7000028341/.

67 Data Retention and Investigatory Powers Act 2014, Act of Parliament, adopté le 18 juillet 2014, http://services.parliament.uk/bills/2014-15/dataretentionandinvestigatorypowers/documents.html.

des données relève du droit de l'Union puisqu'elle intervient en application de la directive 95/46[68] et notamment de l'article 15, paragraphe 1, de la directive 2002/58[69]. Dès lors, les législations des États membres doivent pleinement répondre aux exigences de respect des droits fondamentaux formulées par la Cour dans son arrêt portant sur la conservation des données. Il en ressort que la conservation, de manière globale, indifférenciée des données relatives aux communications électroniques de tous les utilisateurs de ces services sans objectif spécifique, constitue une ingérence disproportionnée dans les droits fondamentaux consacrés par les articles 7 et 8 de la Charte.

Enfin, il est intéressant de noter que dans l'affaire *Maximillian Schrems contre le Data Protection Commissioner*, en réalité contre *Facebook*, la *High Court of Ireland* a posé une question préjudicielle à la Cour portant sur la décision de la Commission 2000/520/CE[70] relative à la protection assurée par les principes de la *sphère de sécurité* (en anglais, « *Safe harbour* »)[71] suite au programme PRISM eu égard aux droits fondamentaux consacrés par les articles 7, 8 et 47 de la Charte. Dans sa décision de renvoi, la *High Court of Ireland* fait référence de manière détaillée à l'arrêt de la Cour dans l'affaire *Digital Rights et Seitlinger* et démontre ainsi clairement que le dialogue des juges en Europe fonctionne aussi dans des domaines hautement politiques et controversés. J'indique que la Cour va rendre son arrêt dans cette affaire cette année.

II. L'arrêt *Google Spain et Google*

Après avoir confirmé l'applicabilité de la directive 95/46 aux activités de *Google* en Europe, la Cour a souligné dans son arrêt *Google Spain et Google*[72], que, conformément à celle-ci, le traitement des données à caractère personnel n'est

68 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.

69 Article 15 § 1 de la directive du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) : « *Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragr. 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragr. 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragr. 1 et 2, du traité sur l'Union européenne* ».

70 Décision 2000/520/CE de la Commission du 26 juillet 2000, 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 posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (JO L 215, p. 7).

71 La sphère de sécurité (en anglais, « *Safe Harbour* ») est un ensemble de principes de protection des données personnelles, négociés entre les autorités américaines et la Commission européenne en 2001.

72 CJUE, aff. C-131/12, 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (dit arrêt *Google Spain et Google*).

permis que lorsqu'il est nécessaire à 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 libertés et les droits fondamentaux de la personne concernée, notamment son droit au respect de sa vie privée[73]. Au vu de la gravité potentielle de cette ingérence dans les droits fondamentaux à la protection de la vie privée et à la protection des données à caractère personnel, la Cour a constaté que cette ingérence ne saurait être justifiée par le seul intérêt économique que tire l'exploitant d'un moteur de recherche de ce traitement. En outre, la Cour a conclu qu'il fallait rechercher un juste équilibre notamment entre l'intérêt légitime des internautes et les droits fondamentaux, consacrés par les articles 7 et 8 de la Charte[74], des personnes concernées. À ce sujet, l'intérêt du public à disposer d'une information peut varier, notamment, en fonction du rôle que joue cette personne dans la vie publique[75]. La Cour laisse également entendre que la nécessaire mise en balance des intérêts en cause peut diverger lorsqu'il s'agit d'un traitement rédactionnel effectué par l'éditeur d'une page Internet[76].

Si l'on prend en considération les structures et les conditions de marché dans lesquelles s'inscrit ce cas de figure, la réalité a largement dépassé la notion bien connue de « *parité contractuelle entravée* »[77]. Pour certains, le fait que l'on se réfère encore aujourd'hui au concept de l'autodétermination informationnelle paraît soit naïf, soit courageux[78]. Le recours à l'accès par voie électronique aux données personnelles dans un but avant tout commercial a effectivement déclenché une dynamique qui menace de déséquilibrer les règles bien établies, au sein des ordres juridiques nationaux, entre la protection de la sphère privée et l'autorisation d'accéder à certaines données pour les utiliser à des fins commerciales. En tout état de cause, il est primordial d'insister sur le fait que l'accès et l'utilisation de données personnelles à des fins commerciales est au cœur des préoccupations de cette évolution.

III. À la recherche d'un fondement conceptuel

Déjà en 1983, la Cour constitutionnelle allemande a saisi l'occasion, dans le cadre d'une affaire portant sur le recensement général de la population, de fonder la protection des données personnelles sur le principe, nouvellement créé, de *l'autodétermination informationnelle*, ce qui fut, à l'époque, une innovation importante qui a été suivie par toute une législation en matière de protection des

73 V. CJUE, aff. C−131/12, 13 mai 2014, *Google Spain et Google*, paragr. 74.

74 Article 7 : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* ». Article 8 : « *Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante* » ; Charte des droits fondamentaux de l'Union européenne.

75 V. CJUE, aff. C−131/12, 13 mai 2014, *Google Spain et Google*, paragr. 81.

76 V. CJUE, aff. C−131/12, 13 mai 2014, *Google Spain et Google*, paragr. 86.

77 Cour constitutionnelle allemande, BVerfGE 89, 214 (234) – Bürgschaftsvertrag.

78 Klar, *Privatsphäre und Datenschutz in Zeiten technischen und legislativen Umbruchs*, DöV 2013, 103, 107 ; Masing, NJW 2012, 2305, 2309 ; Heckmann, *Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz*, NJW 2012, 2631, 2633 ff.

données personnelles. C'est en raison de l'absence de disposition écrite dans la loi fondamentale quant à la protection des données que la Cour constitutionnelle a choisi de reconnaître ce droit à partir d'une lecture combinée des droits de la personnalité et du droit à la dignité humaine, en s'appuyant sur la considération suivante qui me paraît toujours d'actualité : « *l'autodétermination individuelle suppose, même en présence de technologies modernes de traitement de l'information, que l'individu dispose de la liberté de choisir les actions qu'il souhaite entreprendre ou s'abstenir d'entreprendre et de se comporter conformément à ce choix. Le droit à l'autodétermination informationnelle s'oppose à un ordre social dans lequel le citoyen ne serait pas en mesure de savoir qui dispose de quelle information, à quel moment et dans quelles circonstances, le concernant. Cela n'entraverait pas seulement l'épanouissement individuel de chacun mais porterait également atteinte à la société dans son ensemble étant donné que l'autodétermination est une condition de fonctionnement élémentaire pour une communauté démocratique reposant sur la liberté d'action et de participation de ses citoyens* »[79].

En même temps, cette Cour a reconnu que l'individu ne dispose pas d'un droit lui garantissant une maîtrise absolue et illimitée de ses droits, puisque chaque personne vit dans une communauté sociale et interagit avec d'autres individus. Partant, elle a conclu qu'une grande quantité d'informations à caractère personnel démontre une réalité sociale qui ne peut pas être associée à un seul individu. C'est en raison de son intégration sociale que l'individu doit, toujours selon la Cour constitutionnelle allemande, tolérer des limitations de son droit à l'autodétermination informationnelle au profit de l'intérêt général supérieur[80].

À cet égard, il importe de souligner, tout d'abord, que l'autodétermination informationnelle se place dans une perspective de liberté et de dignité de l'individu dans ses relations sociales. Cette conception paraît, en principe, essentiellement inconciliable avec l'idée récente selon laquelle l'autorisation d'accéder à des données à caractère personnel pourrait devenir un moyen important de paiement dans les relations commerciales. Elle se distingue notamment de cette dernière conception en ce qu'elle pose des exigences strictes à un consentement donné pouvant justifier un traitement des données à caractère personnel. L'exemple des bracelets connectés mesurant et collectant en temps réel des données médicales telles que le rythme cardiaque qui peuvent être transmises à des assureurs privés, en contrepartie d'une offre avantageuse, me paraît tout à fait pertinent pour illustrer cette difficulté.

79 Cour constitutionnelle allemande, BVerfGE 65, 1 (42 f.) – Volkszählung : « *Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, dass den Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung (…) nicht vereinbar, in der Bürger nicht mehr wissen könne, wer was wann und bei welcher Gelegenheit über sie weiß. (…) Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfreiheit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist* ».

80 Cour constitutionnelle allemande, BVerfGE 65, 1 (43-44) - Volkszählung.

Ensuite, l'autodétermination informationnelle constitue une conception qui, bien que protectrice, se caractérise par une assez grande souplesse due à une application flexible des exigences de proportionnalité. Par exemple, la prévention du terrorisme a pu justifier l'établissement de profils par le recoupement de données issues de plusieurs sources. De même, l'installation de caméras de vidéosurveillance sur des lieux, même étendus, où la délinquance est importante a été considérée comme justifiée. Par contre, un système général d'enregistrement du trafic permettant d'identifier le numéro d'immatriculation d'un véhicule et l'identité de son conducteur a été jugé excessif en l'absence d'éléments concrets permettant de soupçonner la commission d'un délit sur les lieux en question.

L'exemple de *Google street view* que le Tribunal Fédéral suisse a jugé compatible avec les exigences de l'autodétermination informationnelle, pour autant que certaines conditions notamment relatives à une anonymisation efficace et à l'assurance d'exceptions pour des lieux sensibles et d'espaces privés, prête, à mon avis, à discussion. Je me demande notamment si l'intérêt commercial de *Google* et l'intérêt du public de pouvoir utiliser ce service, qui n'est pourtant pas reconnu par la loi, n'ont pas été privilégiés à tort par rapport à l'intérêt des propriétaires concernés et de la prévention de la délinquance…

Enfin, il me semble que la conception de l'autodétermination informationnelle a parrainé l'élaboration de la directive 95/46, laquelle gouverne toujours la protection des données personnelles en droit de l'Union. Notamment, selon les principes de base contenus à l'article 7 de celle-ci, le traitement des données à caractère personnel est soumis à la nécessité d'une légitimation particulière résultant, par exemple, d'un consentement formellement donné ou d'un intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévalent pas l'intérêt et/ou les droits et libertés fondamentaux de la personne concernée. Le principe directeur du droit de l'Union en matière de protection des données à caractère personnel selon lequel la personnalité et la dignité de la personne concernée par un tel traitement nécessite une protection particulière ressort encore plus clairement de l'interdiction de principe, figurant à l'article 8 de ladite directive, de traiter de telles données si celles-ci révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale de la personne concernée ou si ces données sont relatives à sa santé et à sa vie sexuelle.

Le message clair ressortant des jugements rendus par la Cour de justice de l'Union européenne dans les affaires *Digital Rights et Seitlinger* ainsi que *Google Spain et Google* a été parfaitement entendu. Dans le cadre de ses compétences, la Cour prend ses fonctions très au sérieux et garantit un niveau élevé de protection des droits fondamentaux. Ni plus, ni moins. C'est à d'autres de juger si les arrêts du 8 avril 2014 et du 13 mai 2014 représentent un coup de clairon pour la protection de la vie privée. En protégeant les libertés fondamentales des citoyens européens, la Cour a simplement montré ce qu'est l'office du juge dans une Union de droit.

Jacky Richard

Président adjoint et rapporteur général de la section du rapport et des études.

Merci beaucoup M. le juge von Danwitz pour cet exposé très clair qui montre bien la puissance du concept et ses nuances. Alors, est-ce naïf ou est-ce courageux ? Comme vous, je pense que nous sommes sur la deuxième branche de l'alternative mais le débat ne fait que commencer. Je voudrais demander à Antonio Casilli puis à Délia Rahal-Löfskog de réagir dans un temps limité de trois minutes aux deux interventions. Ensuite, je passerai la parole à la salle.

Antonio Casilli

Maître de conférences à Telecom ParisTech, chercheur au centre Edgar Morin

J'aimerais réagir sur la question de la patrimonialisation qui été évoquée par Me Bensoussan. Il y a plusieurs manières d'entendre le mot patrimoine même si on se situe dans le contexte économique comme vous le faites. Évidemment, on est face à la patrimonialisation au sens de marchandisation, patrimonialisation rampante que vous avez mis en évidence. Par contre, dans d'autres domaines, par exemple en matière culturelle, on parle de patrimoine pour parler d'un ensemble commun, qui ne relève pas de la propriété privée. D'où ma question qui est en fait une manière complémentaire d'envisager notre sujet : *quid* de la possibilité d'un patrimoine collectif ? Que se passerait-il si l'on considérait les données personnelles comme un bien commun ? Il ne s'agirait plus d'envisager ce droit relatif aux données personnelles comme des droits de propriété privée, mais plutôt comme des droits d'accès à un bien collectif.

Alain Bensoussan

Avocat à la Cour d'appel de Paris

Les données à caractère personnel sont des biens incorporels dont la propriété permettrait d'organiser, par analogie aux biens moléculaires, leur protection, les modalités de détention et les échanges de toutes natures, sous réserve des règles d'ordre public.

En la matière, il existe deux grandes décisions. La première est l'affaire *Reno v. American Civil Liberties Union*[81]. La Cour suprême des États-Unis a donné une leçon de démocratie au monde entier en jugeant que l'Internet n'était ni un réseau, ni un protocole, mais un média protégé par le premier amendement. L'ensemble des pays du monde a suivi. La deuxième grande décision, est celle de la Cour de justice de l'Union Européenne à propos de l'affaire *Google Spain*[82], concernant le « *droit à l'oubli* », le fait que chacun d'entre nous puisse, au-delà même de l'autodétermination sur l'usage de ses données, être le seul archiviste de son passé[83].

81 Cour suprême des États-Unis, 26 juin 1997, *Reno vs ACLU*, 521 U.S. 844 (1997).

82 CJUE, aff. C-131/12, 13 mai 2014, *Google Spain SL, Google c. AEPD et Mario Costeja González*.

83 V. A. Bensoussan, « Le droit à l'oubli numérique », 18 mai 2010, répertoire « blog expert Droit des technologies avancées » sur le site du *Figaro*, disponible à l'adresse suivante : http://blog.lefigaro.fr/bensoussan/2010/05/le-droit-a-loubli-numerique.html

Thomas von Danwitz

Président de chambre à la Cour de justice de l'Union Européenne

À un détail près, si vous me le permettez, le citoyen peut utiliser ce type de vocabulaire et parler de mes données mais, en même temps, nous savons très bien que les protocoles techniques d'Internet sont désormais basés sur des logiques que l'on appelle parfois FOAF (« *Friend of a Friend* », en français « *amis d'amis* »), et que si finalement on est constamment connecté à des amis, on est aussi connecté constamment aux données de ses amis. Finalement mes données sont aussi les données de mes amis, car quand je parle de moi je suis en train de dire, dans cent pour cent des cas, quelque chose sur d'autres personnes ! Finalement, cette idée de la personnalisation des données se heurtent à une réalité qui est la réalité sociale de ces données dans le cadre d'Internet.

Jacky Richard

Président adjoint et rapporteur général de la section du rapport et des études

Thomas von Danwitz a parlé du bracelet connecté et a dénié à cette technologie la possibilité de donner accès à des tarifs préférentiels des assureurs qui, ayant des données dont on peut penser qu'elles sont bonnes, pourraient consentir des tarifs préférentiels. C'est une conception de l'assurance qui n'est pas une conception très classique.

Délia Rahal-Löfskog

Chef de service à la santé de la CNIL

Dans le domaine de la santé, les législations successives[84] accordent une place de plus en plus prépondérante à l'autonomie du patient[85]. D'ailleurs, l'individu s'empare de la palette de services offerte par le numérique pour tenter de s'émanciper du traditionnel paternalisme médical. L'accès à l'information a donc immanquablement pour effet de rendre cette autonomie plus effective dans une relation praticien-patient marquée jusqu'alors par une certaine *asymétrie*. Selon une étude intitulée *Les Français et la santé connectée*[86], 56 % des internautes répondants ont indiqué avoir consulté une information de santé sur Internet au cours des six derniers mois, dont 78 % sur un site dédié à la santé.

Dans un univers numérique de plus en plus complexe, certains services placent l'individu, et les données qui lui sont rattachées, au cœur de la relation contractuelle, de sorte qu'il serait tentant de s'orienter vers un droit de propriété sur les données. Pourtant, appliquée aux données relatives à la santé, cette solution trouverait rapidement ses limites.

84 Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé et loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

85 Également appelé selon les terminologies « malade » ou « usager du système de santé ».

86 Étude menée par CCM Benchmark de mars 2014 sur un panel de 1 452 internautes.

En effet, dans le cadre, par exemple, d'une prise en charge médicale, le propriétaire des données serait-il : le patient auxquelles elles sont intimement rattachées, le professionnel de santé qui pose un diagnostic, l'éditeur de logiciel qui fournit le support d'enregistrement de l'information ou encore le réseau social ou le forum de discussions sur lequel le patient/individu a exposé la liste de ses pathologies ?

Outre les difficultés pratiques que cela serait susceptible d'engendrer, s'orienter vers un droit de propriété des données à caractère personnel en matière de santé conduirait nécessairement à repenser la relation entre l'usager et les professionnels, et pourrait avoir pour effet de revenir sur l'autonomie consacrée par la législation et de creuser davantage l'asymétrie entre les deux.

En pratique, cela pourrait par exemple conduire à priver les individus de l'exercice du droit d'accès à leur dossier médical, prévu tant par la loi « informatique et libertés » que par la loi du 4 mars 2002.

Le droit à l'autodétermination informationnelle, tel que préconisé dans l'étude annuelle 2014 du Conseil d'État, contribuerait donc à replacer l'individu au cœur de la question des données personnelles. Également promu par la CNIL à travers sa demande de reconnaissance d'une constitutionnalisation de la protection des données personnelles, ce droit permettrait d'élever la protection dévolue aux individus et aux données qui les concernent, étant précisé, tel que souligné par le Conseil d'État, que ce droit doit se lire comme *« un principe donnant sens »* aux autres droits reconnus à l'individu par la protection des données personnelles et *« devant être interprétés et mis en œuvre à la lumière de cette finalité »*.

Par ailleurs, la consécration d'un droit à la portabilité, tel qu'envisagé par le règlement général relatif à la protection des données actuellement en discussion au Parlement européen, donnerait une nouvelle impulsion à la mise en œuvre de ces droits.

En matière de santé, le droit à la portabilité de ses données pourrait, par exemple, constituer une sorte de pendant de la liberté de choisir son médecin ou son établissement de santé[87], sans avoir à réaliser, une nouvelle fois ou systématiquement, l'ensemble des examens médicaux.

La question de l'asymétrie reste au cœur de la relation entre l'individu et les opérateurs du numérique. Face à la massification des données et au gigantisme des bases, au-delà de la reconnaissance d'un droit à l'autodétermination informationnelle, d'autres réponses juridiques pourraient permettre de rééquilibrer la relation.

À cet égard, l'ouverture de l'action de groupe au droit des données personnelles pourrait, à l'instar des dernières évolutions législatives en faveur du droit de la consommation[88] ou du droit de la santé[89], s'avérer une réponse efficace. Ceci est d'autant plus vrai aujourd'hui avec l'essor des objets connectés (montres,

87 Reconnu principe fondamental de la législation sanitaire par l'article L. 1110-8 du code de la santé publique.

88 Loi n° 2014-344 du 17 mars 2014 relative à la consommation.

89 Projet de loi de modernisation de notre système de santé, en discussion au Parlement au moment de la rédaction de ces lignes.

podomètres, capteurs de fréquence cardiaque, tensiomètres, etc.) dont le grand public est friand. Outre la question du statut de la masse de données générées par ces objets ou dispositifs, se pose la question du risque pour les individus quant à l'utilisation, choisie ou subie, de leurs données.

Jacky Richard

Président adjoint et rapporteur général de la section du rapport et des études

J'ai une question pour Mme Rahal-Löfskog provenant de la salle d'à côté où sont projetés nos débats sur écran pour l'auditoire qui n'a pas pu être installé en salle d'Assemblée générale : « *Ne faut-il pas envisager une redéfinition des données personnelles pour y ajouter les agrégats de données non personnelles, des données en soi mais personnelles après coup, surtout pour les données de santé ?* ». Je viens de me concerter avec cette dernière qui va y répondre dans le cadre de son exposé.

Délia Rahal-Löfskog,

Chef de service à la santé de la CNIL

L'intérêt de traiter des données dites « *de santé* » peut trouver de nombreuses illustrations. Parmi les domaines qui relèvent de la compétence de la CNIL, celui de la recherche médicale est le plus prolifique. Ainsi, la CNIL autorise, chaque année, plus de sept cents projets de recherche médicale, sans compter les études dites « *monocentriques* »[90].

Outre l'intérêt direct pour l'individu de voir conduites des recherches afin de mieux comprendre la ou les pathologie(s) dont il souffre, il existe indéniablement un intérêt de santé publique à apporter les réponses thérapeutiques appropriées ou à mettre en place des actions préventives permettant de limiter les effets des pathologies et qui pourraient bénéficier à l'ensemble des personnes malades.

C'est en raison de cet intérêt public que la CNIL œuvre pour favoriser la recherche dans le domaine de la santé et qu'elle peut autoriser, moyennant des garanties appropriées, la mise en œuvre de grandes cohortes dont certaines conduisent à suivre les personnes depuis leur plus jeune âge jusqu'à l'âge adulte.

Cependant, en cédant à la tentation de ne pas informer les personnes concernées, au nom de l'intérêt supérieur de la découverte d'un remède par exemple ou de mieux comprendre les conditions de survenue d'une pathologie, le promoteur d'une recherche expose la validité de sa recherche qui n'aurait pas été conduite dans des conditions conformes à la loi[91].

Il existe également un intérêt certain à ce que les données relatives à la santé d'une personne puissent être partagées entre les professionnels ou établissements de santé qui interviennent dans le cadre de sa prise en charge, dans un objectif de coordination des soins. C'est, par exemple, le cas pour la mise en œuvre de réseaux de soins partagés, ou en matière de télémédecine, dont le but premier est

90 Les études monocentriques relèvent du régime de la déclaration normale prévue à l'article 22 de la loi du 6 janvier 1978 modifiée.

91 Outre les sanctions issues de la méconnaissance de la loi « informatique et libertés ».

de lutter contre la désertification médicale et ainsi permettre une prise en charge plus rapide des malades dans des territoires dont la couverture sanitaire ne le permettrait pas.

Le traitement de données de santé individuelles peut donc satisfaire l'intérêt direct de la personne concernée comme celui de la collectivité. Il comporte cependant des risques qui doivent être mesurés et identifiés, afin que des garanties appropriées soient mises en œuvre pour maintenir l'équilibre indispensable à l'écosystème numérique.

Parmi les principaux risques pour l'individu, celui de la divulgation non autorisée de données inhérentes à l'intimité de sa vie privée, alors même que celles-ci ont pu être collectées dans le cadre de sa prise en charge ou afin de l'aider à mieux connaître la pathologie dont il souffre.

Compte tenu de la nature particulièrement sensible des données relatives à la santé, les conséquences de cette divulgation non autorisée peuvent engendrer un préjudice difficilement réparable, tant pour l'individu directement concerné que pour son entourage, en particulier dès lors qu'il s'agirait de pathologie(s) héréditaire(s) ou génétique(s).

Pour le responsable de traitement, le risque est de nature juridique : s'agissant du partage d'information entre plusieurs acteurs dans le cadre de la coordination des soins par exemple, le numérique a pour effet d'augmenter le risque d'accès non autorisé à des informations couvertes par le secret, engageant ainsi la responsabilité des débiteurs de cette obligation de secret. Cet accès non autorisé peut trouver son origine dans des actes malveillants (relevant de la cybercriminalité), mais peut également être le résultat de négligence comme celle consistant, par exemple, à ne pas sécuriser un site Internet par l'utilisation d'un protocole « *https* »[92].

À titre illustratif, l'absence de sécurisation d'un site de stockage d'imagerie médicales conduisant à la diffusion des clichés radiographiques d'une personne souffrant d'une maladie grave ont pu être indexés par un moteur de recherche et ainsi être accessibles à son entourage alors que la personne concernée avait choisi de ne pas révéler sa maladie.

Il convient dans ce cas que l'opérateur mette en place, sans délai, les mesures correctives adéquates. Il n'en demeure pas moins que cette rupture dans la chaîne de confidentialité peut avoir des répercussions graves sur la vie privée des personnes concernées.

Dans le cadre de l'exercice de sa mission de régulateur, la CNIL participe à l'élaboration de référentiels de sécurité des systèmes d'information en santé, et met à la disposition des professionnels (éditeurs de logiciels notamment) des recommandations leur permettant d'élever le niveau de sécurité des logiciels qu'ils commercialisent. Elle a également adopté une autorisation unique relative à la messagerie sécurisée de santé[93] qui fournit un cadre juridique et technique

92 Le *protocole de transfert hypertexte sécurisé* (*https*) est la combinaison du « *http* » avec une couche de chiffrement comme les protocoles de sécurisation des échanges SSL ou TLS.

93 Délibération n° 2014-239 du 12 juin 2014, publiée au JO du 16 juillet 2014.

conforme aux exigences de la loi et à l'état de l'art, afin que l'échange de données médicales, entre professionnels qui participent à la prise en charge d'un individu, s'opère dans des conditions adéquates.

En outre, l'essor des objets connectés donne une nouvelle dimension au risque et nécessite de repenser le mode de régulation afin de voir émerger un cadre de confiance où les intérêts de l'ensemble des parties prenantes sont préservés. Le régulateur est, à cet égard, convaincu qu'il est possible de concilier innovation technologique et protection des données personnelles.

La CNIL a d'ailleurs engagé une réflexion prospective qui a notamment donné lieu à la publication de travaux sur le sujet[94]. Un certain nombre de scénarios[95] y sont développés et sont une projection de ce que pourrait être l'utilisation, sans encadrement, de certains objets connectés.

Compte tenu de l'encadrement juridique spécifique des données relatives à la santé notamment par la loi « informatique et libertés »[96], une des principales questions est celle de la qualification : une donnée produite par un objet connecté dit « *à usage domestique* » revêt-elle la qualification de donnée dite « *de santé* » ou de donnée de bien-être ? Le sujet n'a de simple que l'apparence. La complexité naît de la diversité des objets et de leurs fonctionnalités, d'une part, et de l'imbrication des usages (médicaux ou personnels), d'autre part.

Ainsi, les données issues de l'utilisation d'un tensiomètre ou d'une montre qui mesure la fréquence cardiaque doivent-elles être qualifiées de données de santé ou de données de bien-être ?

Le poids et la taille en tant que tels ne paraissent pas, par essence, relever de la qualification de données relatives à la santé. En revanche, le croisement des informations relatives au poids et à la taille permet de déduire des informations sur l'état de santé. Si à ces informations, s'ajoutent celles relatives à la circonférence abdominale et au nombre de pas effectués par un individu au quotidien, il est possible d'en déduire, au regard des études scientifiques publiées, un risque cardiovasculaire plus ou moins élevé.

Il ressort de la jurisprudence du Conseil d'État[97] que les données qui permettent d'identifier immédiatement la nature de l'affection ou du handicap propre à une personne doivent être regardées comme des données personnelles relatives à la santé.

94 CNIL, Cahier IP Innovation & prospective n° 2, *Le corps, nouvel objet connecté*, mai 2014 (V. aussi Cahier IP Innovation & Prospective n° 1, *Vie privée à l'horizon 2020, Paroles d'experts*, novembre 2012).
95 La collection *Cahiers IP, Innovation & prospective* présente les études prospectives conduites par la direction des études, de l'innovation et de la prospective de la CNIL, créée en 2011, et par son laboratoire d'innovation, afin de contribuer à nourrir le débat et la réflexion dans le champ informatique et libertés.
96 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (JORF, 7 janvier 1978, p. 227) modifiée 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 (JORF, 7 août 2004, p. 14063) et par la loi n° 2014-344 du 17 mars 2014 relative à la consommation.
97 CE, 19 juillet 2010, *M. Fristot et Mme Charpy*, req. n° 317182.

La Cour de justice de l'Union européenne[98] considère qu'il y a lieu d'avoir une interprétation extensive de la notion de « *données relatives à la santé* », de sorte qu'elle comprend tous les aspects tant physiques que psychiques de la santé d'une personne. Cette acception large est également reprise dans le projet de règlement général sur la protection des données actuellement en cours de discussion.

La qualification des données issues des objets connectés a également un impact sur l'encadrement de ces objets, notamment pour savoir s'ils relèvent de la catégorie des dispositifs médicaux ou de la réglementation sur l'hébergement de données de santé prévue par le code de la santé publique[99]. En outre, l'usage de l'objet (par exemple, la transmission par une application ou un objet connecté des informations relatives à l'indice glycémique d'un individu à son médecin) peut conduire à faire application des dispositions relatives à la télémédecine[100].

Se pose aussi la question cruciale de l'information des personnes sur les destinataires des données que ces dispositifs collectent, sur l'usage qui en est fait ainsi que sur les conditions de stockage de celles-ci.

Cette question revêt une importance cruciale pour le régulateur car l'enjeu est celui de la compréhension de l'étendue de l'engagement de chacun quand il connecte son corps au réseau.

Jacky Richard

Président adjoint et rapporteur général de la section du rapport et des études

Avant les questions, je souhaiterais que l'on enchaîne sur l'exposé de M. Casilli qui a beaucoup travaillé sur la conception de la vie privée dont la configuration, les limites, les contraintes et les potentialités sont considérablement modifiées du fait de la multiplication des données à caractère personnel numérisées.

Antonio Casilli

Maître de conférences à Telecom ParisTech, chercheur au centre Edgar Morin

Je vous remercie de votre invitation à participer à cette journée de mise en débat des propositions contenues dans l'étude annuelle 2014 du Conseil d'État *Le numérique et les droits fondamentaux*, étude que j'ai accompagnée en qualité de membre du groupe de contact et à laquelle j'ai contribué avec un texte[101].

Pour comprendre le rôle et la place des données dans le contexte sociotechnique contemporain il faut, d'abord, prendre en compte la relation théorique existante entre vie privée *et* données personnelles. Les termes mêmes que nous employons pour définir ces entités (à la fois légales, techniques et politiques) s'avèrent ambivalents. Dans des réseaux numériques où chacun d'entre nous est conçu

98 CJCE, aff. C-101/01, 6 novembre 2003, *Bodil Lindqvist*.

99 Article L. 1111-8 du code de la santé publique.

100 Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine.

101 A. Casilli (2014) « Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée » in Étude annuelle 2014 du Conseil d'État, *Le numérique et les droits fondamentaux*, La Documentation française, pp. 423-434.

comme un FOAF en puissance (« *Friend of a Friend* », en français « *ami d'ami* »), il est évident que nos données sont aussi, dans une certaine mesure, des DOAF (« *Data of a Friend* », en français « *données d'ami* »). Toute information personnelle dévoilée ou capturée sur notre compte, dévoile et capture la vie, les opinions et les agissements des autres membres de notre profil social sur Internet.

Il n'y a aujourd'hui rien de plus collectif qu'une donnée personnelle et rien de plus public que l'ensemble des enjeux soulevés par la vie privée. Et pourtant, le débat qui porte sur ces entités est confisqué depuis des décennies par un lieu commun, vieux comme l'Internet même : l'annonce de la fin de la vie privée.

La vie privée, on l'enterre depuis désormais deux décennies

Depuis désormais vingt ans, avec une régularité de métronome, on enterre la vie privée. Et à chaque fois ses funérailles se terminent par une photo de groupe (la dernière a été prise au Forum économique mondial de Davos) où figurent tous les industriels qui profitent du marché des données personnelles, les hommes politiques qui invoquent des lois qui restreignent les libertés, les journalistes médiocres qui stigmatisent les utilisateurs de technologies numériques tout en ignorant les rudiments de l'informatique.

Force est de constater que chaque enterrement devient aussi l'occasion pour compter le nombre croissant d'activistes et de citoyens de plus en plus déterminés et influents qui militent pour la défense de cette vie privée qu'on voudrait morte, mais qui refuse finalement de mourir. Pour paraphraser une chanson d'Eugène Pottier, « *À l'enterrement d'la vie privée, on était un fier tas à lui servir d'escorte. Ce qui prouve en tous cas que la vie privée n'est pas morte (…)* ».

C'est une suite romanesque, voire un cycle épique, que nous vivons : on annonce la mort de la vie privée, on admet qu'elle est ressuscitée, on la fait mourir à nouveau, etc. Donc, la vie privée ne meurt pas : elle change. Et le clivage qui existe entre notre image surannée et sa réalité contemporaine détermine cette suite d'erreurs, cette confusion. Faisons alors un effort de compréhension.

Je commencerai par vous demander de m'accorder un postulat : *avant même d'être une valeur, la vie privée est une force sociale*. En tant que telle elle s'oppose à d'autres forces qui cherchent à l'affaiblir ou alors, dans la *novlangue* des gouvernements sécuritaires occidentaux, « *à l'équilibrer* ». L'autre pilier de cet « *équilibre indispensable* » serait, tour à tour, la sécurité, l'innovation, la transparence, etc. Voilà toutes les autres forces sociales que le Premier ministre a eu la gentillesse de répertorier pour nous à l'occasion du *European Data Governance Forum* du 8 décembre 2014.

La notion de la vie privée a changé : nous sommes passés de la vie privée pénétrable à la vie privée négociable

Si cette rhétorique trompeuse de la *fin de la vie privée* est difficile à dissiper, c'est parce que notre manière d'envisager la vie privée a changé, à tel point qu'elle

est devenue méconnaissable[102]. Nous avons hérité du XIXe siècle une notion de vie privée en tant qu'entité monodirectionnelle, centrée autour d'un noyau dur d'informations sensibles. Cette vision, désormais inadaptée au contexte technologique actuel, mais sur laquelle les législations contemporaines sont encore basées, nous met dans une situation politiquement explosive.

Quand la jurisprudence s'était saisie pour la première fois de la question en 1890, le droit à la vie privée avait été défini par Louis Brandeis et Samuel Warren comme « *the right to be left alone* » (en français « *le droit d'être laissé en paix* »). Avant Internet, la notion de vie privée pouvait être qualifiée de « *privacy as penetration* » (en français « *vie privée comme pénétrable* »). La sphère privée serait un ensemble de données concentriques qui entourent un noyau dur d'informations sensibles. C'est une hiérarchie rigide d'informations, allant des plus notoires, connues par autrui, jusqu'aux plus intimes et nécessitant d'un maximum de protection.

Ce modèle, pour autant qu'il représente une situation idéale, n'a plus de sens dans un contexte de connectivité généralisée. Sur Internet, personne n'a envie d'être laissé en paix, de vivre une vie dans l'isolement. Au contraire, nos technologies sociales sont accompagnées par la promesse d'une vie relationnelle riche et brillante.

La vie privée aujourd'hui est plutôt caractérisée par le besoin de *maitriser l'information qui circule sur notre compte*, son accès, ses modalités de partage. Chaque fois que nous téléchargeons une application sur nos téléphones, que nous nous inscrivons sur un nouveau site Internet, nous formulons un ensemble d'attentes implicites ou explicites, lesquelles – lorsqu'elles sont trahies par les propriétaires des services ou par les pouvoirs publics censés les faire respecter – déterminent à nos yeux autant de « *violations de la vie privée* ».

La vie privée est désormais la « *privacy as negociation* », une négociation basée sur la recherche d'un accord entre plusieurs parties, plus que sur une régulation émanant d'une seule d'entre elles. Les acteurs recherchent une consonance, confrontent leurs intérêts, sont prêts à des concessions mutuelles en termes de dévoilement et d'accès à des informations potentiellement sensibles.

La perte de vie privée sur certains éléments n'équivaut pas à une débâcle incontrôlée, mais plutôt à une retraite stratégique sur les points où la négociation est difficile. On accepte de ne pas déployer des efforts imposants quand on sait que l'on n'a pas beaucoup de chances de réussir, mais on concentre les efforts ailleurs, par exemple sur la création de privilèges différenciés d'accès au profil en autorisant seulement certains individus à atteindre certains contenus, ou sur la création de faux profils « *anonymes* » pour chercher à maîtriser ce qui est associé à l'identité civile de l'utilisateur, ou sur la publication de « *notices de vie privée* », ces messages certes inefficaces mais symptomatiques d'une volonté des utilisateurs de réaffirmer qu'ils détiennent un droit personnel sur les éléments partagés.

102 V. A. Casilli « Contre l'hypothèse de la fin de la vie privée. La négociation de la *privacy* dans les médias sociaux », *Revue française des sciences de l'information et de la communication*, 2013.

La négociation n'est pas la marchandisation des informations personnelles

Le mot « négociation » a pu paraître, aux lecteurs moins attentifs de mes travaux, un synonyme de « monétisation ». Cela évidemment fait écho aux discours portés par les acteurs de l'économie numérique. Déjà en 2011, le *World Economic Forum* décrivait les données personnelles comme des catégories d'actifs émergents. La tentation de mettre en place un marché des données personnelles, où chacun pourrait céder des *morceaux de vie privée* moyennant le paiement d'un montant spécifié, doit être combattue. D'où l'urgence de réaffirmer ma position à cet égard : je suis résolument contre la *privatisation de la vie privée*, c'est-à-dire la réduction des données personnelles à des objets de propriété privée.

Le Conseil d'État, dans son étude annuelle 2014, s'est prononcé contre l'instauration d'un tel droit de propriété privée et, la même année, le Conseil national du numérique français avait invoqué dans un rapport sur la neutralité du net le besoin d'équilibrer « *le rapport de force entre consommateurs et entreprises* » : la vente de données sous un régime de propriété privée ne pourrait alors générer que « *des revenus anecdotiques* » et déboucherait sur un renforcement des inégalités entre citoyens.

Dans le contexte actuel, la vie privée ne peut plus être une transaction où chaque individu serait seul face aux autres, mais une concertation où les motivations des citoyens se combinent pour créer des collectivités sociales (groupes de pression, associations spécialisées, instances reconnaissables de porteurs d'intérêts) qui engagent une confrontation avec les organisations industrielles et les pouvoirs étatiques.

Dans ma conception, la négociation de la vie privée se vit avant tout comme une négociation collective, conflictuelle et itérative, visant à adapter les règles et les termes d'un service aux besoins de ses utilisateurs. Le processus de détermination des conditions d'usage est jalonné par une série de batailles que les acteurs publics ont encore du mal à appréhender – mais que les propriétaires de grandes exploitations de données et les concepteurs de plateformes de socialisation en ligne sont encore loin d'avoir gagnées.

De même, ces batailles sont loin d'être gagnées par les pouvoirs exécutifs cherchant constamment à brider la force de négociation de la société civile en diabolisant les usages numériques, et en créant des paniques morales autour des pratiques citoyennes de protection de la vie privée sur Internet.

Vers un nouveau cycle de vie privée post-Charlie, Internet triste ?

Pour revenir à cette vie privée dont on annonce périodiquement la disparition, et pour prendre en compte la nature récurrente de cette annonce, dans notre livre *Against the Hypothesis of the End of Privacy*[103], mes co-auteures Paola Tubaro, Yasaman Sarabi et moi-même, avons avancé une explication en termes de « *cycles de vie privée* ».

103 *Against the Hypothesis of the End of Privacy. An Agent-Based Modelling Approach to Social Media*, P. Tubaro, A. Casilli, Y. Sarabi, ed. Springer, 2014.

Ce que l'on observe du comportement des utilisateurs des médias sociaux généralistes est illustratif à cet égard. Au moment de l'inscription aux plateformes de socialisation numérique, la valeur de la *prédisposition moyenne à la protection de la vie privée* (mesurée en agrégeant plusieurs indicateurs relatifs à une variété d'informations personnelles) diminue d'abord légèrement, quitte à augmenter fortement par la suite. Malgré un abandon initial de la vie privée (nécessaire aux utilisateurs pour se familiariser avec la plateforme et pour cumuler un capital social en ligne fait d'expérience, de réputation et de visibilité), une contre-tendance s'entérine : les utilisateurs de médias sociaux commencent à se surprotéger quand ils sentent que trop d'éléments de leur sphère privée sont menacés d'une perte de maîtrise.

Après l'analyse de séries historiques des conflits autour de la vie privée, nous avons pu démontrer que le dévoilement de soi est loin d'être une tendance linéaire. Les révélations (telles celles d'Edward Snowden depuis 2013), les failles de sécurité (comme celles qui émaillent l'histoire des médias sociaux depuis 2005) ou les annonces tonitruantes de nouvelles « *mesures exceptionnelles* » draconiennes et contreproductives (comme les toutes récentes voulues par le ministre de l'intérieur français) provoquent des dynamiques de surprotection des données personnelles qui contrebalancent ces événements perçus – à juste titre – comme des menaces pesant sur la vie privée des citoyens. Parfois cette surprotection passe par l'ajustement des paramètres de confidentialités des plateformes, parfois par l'usage d'outils avancées (*cf*. à cet égard la popularité croissante du chiffrement), parfois par l'adoption de comportements qui tombent dans une zone grise entre stratégies informelles et usages interdits par les plateformes.

Ces réactions et contre-réactions déclenchent une allure cyclique pour la vie privée qui commence à osciller entre des valeurs extrêmes vers le haut (surprotection) et vers le bas (ouverture forcée des profils utilisateurs voulue par les gouvernements ou par les entreprises privées).

Ce qui nous permet de mieux comprendre le sens de notre postulat initial : certaines forces sociales poussent pour remettre le compteur de la vie privée à zéro, les citoyens-utilisateurs réagissent en réglant au maximum leur protection, et ainsi de suite dans des fluctuations potentiellement infinies. Les interventions des entreprises du numérique ou des gouvernements dans ce sens ne sont pas seulement de courte durée : elles produisent l'effet inverse de celui escompté.

Le paradoxe de la vie privée n'est pas que tout le monde l'invoque et que si peu d'acteurs publics ou privés agissent réellement pour la défendre. Le paradoxe réel, que démontrent nos travaux, est que l'intervention même des gouvernements et des fournisseurs de services de réseaux sociaux déchaîne les réactions de sensibilisation à la prise en compte de la valeur sociale des données personnelles des utilisateurs.

Aujourd'hui, après la vague d'attentats qui a secoué plusieurs pays – le Canada en octobre 2014, l'Australie en décembre 2014 et la France au mois de janvier 2015 – nous constatons ce changement de paradigme. Nous sommes ainsi entrés dans un

nouveau cycle, que nous pourrions qualifier de *cycle Post-Charlie, Internet triste* : après les assassinats, Internet et les libertés numériques sont devenus les boucs émissaires des paniques morales les plus extrêmes et poussent le conflit autour de la protection de la vie privée à un autre niveau. Les explosions de rhétorique sécuritaire, les invocations d'un « *Patriot Act à la française* », la possibilité d'une surveillance numérique de masse encore plus inscrite dans la loi qu'aujourd'hui ne constituent pas des exceptions. Ils ne font que déclencher un autre cycle de cette négociation collective qui oppose les gouvernements, les acteurs privés, les collectifs de citoyens et les nouvelles instances de gouvernance qui apparaissent au niveau locale dans une accélération centripète qui nous rapproche de plus en plus de cette valeur centrale qu'est notre vie privée.

Jacky Richard

Président adjoint et rapporteur général de la section du rapport et des études

Merci beaucoup au chercheur, au sociologue et au fin observateur des évolutions de la société que vous êtes.

Alain Bensoussan

Avocat à la Cour d'appel de Paris

Je souhaiterais faire une remarque sur la notion de vie privée et ses limites. La vie privée, et M. Casilli a eu raison de citer l'article fondateur d'Harvard, est protégée aux États-Unis par le quatrième amendement. Or la géolocalisation, quant à elle, ne tombe pas sous le coup du quatrième amendement.

Certes, on peut réinterpréter la notion de vie privée, mais cela pose deux problèmes : la notion de zone géographique qui n'a plus de sens, et la personnalisation anonyme qui devient de plus en plus importante. Aujourd'hui, le centre de gravité n'est plus sur l'individu mais dans le chaudron des mégadonnées, dans la matrice où tout se calcule de façon collective et anonymisée.

Aujourd'hui, avec seulement cinq informations, il est démontré que l'on peut identifier toute personnalité. La *personnalisation anonyme* est donc le nouveau concept qui entre en conflit avec la vie privée : je ne connais pas cette personne mais pourtant je sais qu'elle aime le jazz et donc aimera les romans policiers ; je sais donc comment elle va se comporter lorsque je vais lui proposer un tel produit.

Il y a ici en jeu deux droits fondamentaux attachés au respect de la vie privée. Le premier, est le *droit de révélation*, c'est-à-dire que la matrice en sait plus que moi sur mes goûts et je suis incapable d'anticiper ses calculs qui me catégorisent. De sorte que, pour mon malheur, il existe 90 % de chance que je réponde favorablement à ses avances. Il y a donc ici une obligation de révélation, et non pas d'accessibilité. Le deuxième droit fondamental, est le *droit de proportionnalité*. Si cinq informations suffisent pour disposer d'un profil numérique conforme de

l'individu au plus profond de lui-même, il faut, pour se protéger, pouvoir disposer d'un droit de proportionnalité, c'est-à-dire d'un droit d'arrêter le traitement de la connaissance par l'algorithme.

M. Casilli a raison de reposer ces questions. Ce n'est pas une critique de la loi « *informatique et libertés* », ni des droits et des libertés; il s'agit de montrer que la technologie des mégadonnées oblige à repenser la notion de vie privée, non plus en termes de zones mais de traitement des données dans une matrice.

Thomas von Danwitz
Président de chambre à la Cour de justice de l'Union Européenne

Je suis également foncièrement d'accord avec les constats de M. Casilli. Je trouve qu'effectivement le vrai défi est cette transformation de la vie privée, et l'étude 2014 du Conseil d'État le démontre. La tâche du législateur est d'encadrer cette transformation, de trouver des règles spécifiques à cette transformation de la vie privée, mais, évidemment, et c'est ma position de base, en gardant les valeurs fondamentales de la vie privée.

Échanges avec les participants

Question *– Est-ce que le débat se déroule dans les mêmes termes aux États-Unis ?*

Alain Bensoussan

Aux États-Unis, la protection des données personnelles se joue au niveau du droit de la consommation. C'est un premier élément qui fait que l'on est moins sur le terrain des libertés publiques et plus sur celui de la liberté du commerce et du droit de la consommation, comme par exemple le droit à la portabilité des services de téléphonie et d'Internet. Le deuxième élément est que l'aspect technologie est plus prégnant, et qu'il fait l'objet d'une régulation pragmatique de son usage. Le troisième élément de dissociation est que le débat sur la propriété est particulièrement important en Californie, notamment à travers une réflexion sur le vol de biens immatériels. Lorsque le transfert des données se fait à travers Internet, comme par exemple via les « Dropbox »[104], les cours américaines ne reconnaissent pas pour l'instant le vol d'informations malgré la pression des utilisateurs. Il faut encore attendre, car en matière de libertés fondamentales c'est souvent par le droit pénal que les libertés civiles s'inscrivent dans le présent.

104 *DropBox* est un logiciel permettant à l'utilisateur de stocker, de partager et de synchroniser ses fichiers par Internet.

Jacky Richard

Sur cette dimension comparative, vous avez quelques pages dans l'étude annuelle 2014 du Conseil d'État. Pour prolonger ce qui vient d'être dit, il n'existe pas dans le droit américain de cadre général protecteur comme dans le droit européen. On est davantage dans une approche subjective de la réparation du préjudice subi qui en effet s'apparente plus au droit de la consommation.

***Question** – La question est pour M. von Danwitz. Dans l'étude annuelle 2014 du Conseil d'État, il existe un doute existentiel sur l'interprétation de l'arrêt de la Cour sur la rétention des données, entre une interprétation minimaliste, qui verrait dans l'arrêt une simple mise en garde sur le manque de proportionnalité des mesures, des inquiétudes auxquelles il pourrait être répondu en apportant des garanties en termes de conditions d'accès aux données, de durée de rétention des données par les opérateurs Télécom, et une interprétation plus maximaliste qui est celle portée par des acteurs de la société civile voyant l'arrêt de la Cour comme avalisant le principe même d'une surveillance de masse des populations, y compris en l'absence de suspicion. Le Conseil d'État penche sur l'interprétation minimaliste en apportant des garanties, notamment en droit français, sur les conditions d'accès aux données des opérateurs. Si l'interprétation maximaliste venait à être confirmée par la CJUE, le Conseil d'État suggère dans son rapport l'adoption d'un protocole interprétatif de la Charte pour consacrer au niveau du droit positif l'acceptation du principe d'une surveillance de masse généralisée. D'où ma question : d'un point de vue personnel, est-ce que vous avez une opinion sur l'une ou l'autre des interprétations, et quelle serait celle de la Cour si elle devait se prononcer à l'avenir sur cette question ?*

Thomas von Danwitz

C'est une question que l'on me pose assez régulièrement. Il y avait même des ministres en visite à la Cour qui posaient cette question parce qu'effectivement, la plupart des États membres sont confrontés à la question de savoir que faire des lois de transposition qu'ils ont élaborées.

D'abord, la Cour parle par ses arrêts et non à travers les déclarations personnelles de ses juges ; et ce sont bien ces œuvres collégiales et collectives qu'il faut respecter dans leur ensemble. Ensuite, sur le fond de votre question, si l'on étudie bien cet arrêt – le Conseil d'État l'a certainement bien fait –, il faut savoir que nous étions confrontés à une situation dans laquelle la directive était marquée par une généralisation des données à collecter et à conserver, à savoir toutes les « métadonnées » des moyens de communication électroniques : non seulement les adresses IP et les communications mobiles, mais également toutes les technologies : fixe, mobile et internet. Et tout cela, pour l'ensemble de la population et pour une durée indéterminée, sans besoin de craindre l'implication même indirecte ou très improbable de quelqu'un dans la commission d'une infraction.

***Question** - Fondateur du moteur de recherche français* Innooo[105]*, ma question est la suivante : pensez-vous qu'en termes de santé et de données personnelles, le droit à l'autodétermination soit plus adapté que le droit de propriété ? Pensez-vous que le droit à l'autodétermination soit plus moral que le droit de propriété ?*

Délia Rahal-Löfskog

La CNIL est d'avantage favorable au droit à l'autodétermination dont elle soutient la reconnaissance, tout comme elle demande la constitutionnalisation de la protection des données à caractère personnel, pour élever davantage le niveau de protection des données personnelles.

Antonio Casilli

Difficile de répondre sur la moralité intrinsèque de l'autodétermination ou de la propriété. Je chercherai à pointer deux éléments intéressants dans chacun des deux concepts. Le premier est que l'autodétermination informationnelle, quand on l'applique au contexte des usages numériques actuels, a besoin d'au moins un protocole d'application pour comprendre la signification de cette formule. Finalement, que veut dire autodétermination s'agissant de données stockées dans un téléphone portable ? Est-ce de savoir ce que contient la base de données ? Comprendre quels sont les algorithmes qui permettent le traitement de certaines informations ? En l'état actuel des choses, cela a encore besoin d'être analysé.

Concernant la propriété, plusieurs éléments de réponse sont contenus dans le rapport 2014 du Conseil national du numérique sur la neutralité des plateformes[106]. Ce rapport indique que si l'on mettait en place un régime de marchandisation des données personnelles, au vu des asymétries actuelles du marché, cela se solderait pour les utilisateurs par des gains anecdotiques et un renforcement des inégalités sociales. Finalement, on se trouverait avec des personnes qui seraient obligées d'accepter des marchés de dupes sur leurs propres données personnelles. Dans ce contexte, la propriété privée des données personnelles peut être envisagée comme « moins morale », mais je le mets vraiment entre guillemets.

***Question** - Je voudrais revenir sur le droit à l'oubli : est-ce considéré comme un droit fondamental ? Est-ce que la loi prévoit des outils pour faire fonctionner ce droit ? Est-ce possible techniquement ? Nous avons évoqué les cycles d'identité, je pense notamment à l'usage qu'ont les adolescents des réseaux sociaux. Nous avons également évoqué le concept de matrice, peut-on imaginer s'en servir pour connaître à l'avance le résultat d'une élection ?*

105 *Innooo* (INNOvation Ouverte Online).

106 Rapport du Conseil national du numérique, *Neutralité des plateformes, réunir les conditions d'un environnement numérique ouvert et soutenable*, remis au ministre de l'Économie, du Redressement productif et du Numérique et à la secrétaire d'État chargée du Numérique, mai 2014.

Alain Bensoussan

Un premier élément est le droit à l'oubli qui, comme l'a remarqué M. von Danwitz, pose une vrai question de proportionnalité. Le droit à l'oubli est une combinaison entre le fait que chacun d'entre nous puisse diffuser certaines informations tout en préservant son propre jardin secret. Le deuxième élément est le travail sur la mémoire que permettent les nouvelles technologies de l'information et de la communication. Et le troisième élément, c'est l'autodétermination, le fait que l'on veuille parfois oublier ce que l'on a fait, avec l'amnistie ou le droit au pardon.

Cela veut dire qu'il faut trouver des points d'équilibre et que chacun d'entre nous puisse en être maître. Il convient de souligner la mise en place par Google d'un comité d'éthique. Finalement, le droit à l'oubli est un droit qui doit être pris en charge par chacun d'entre nous, cela fait partie des libertés fondamentales.

Quant à la matrice où les données sont traitées, je ne sais pas si l'on peut en sortir des résultats prospectivistes pour les élections… Mais il est sûr que chacun d'entre nous envoie de multiples signaux, même faibles, sur ses affinités, notamment politiques. Il y a par exemple, l'utilisation du bouton « j'aime » ; si l'on recoupe ces « j'aime », on trouve un profil, des corrélations, et l'on peut alors faire des analyses sur votre personnalité. Cela n'a rien d'anormal ou d'illégal, mais il faut définir ensemble des points d'équilibre entre le droit de calculer un profil et le droit, pour chacun d'entre nous, d'être maître de son profil.

Thomas von Danwitz

L'arrêt Google and Google Spain *était certes audacieux, mais je dois quand même dire que nous sommes restés dans le rôle classique d'un juge, c'est-à-dire que nous n'avons pas décrété un droit à l'oubli.*

C'est pourtant la formule que la presse a retenue, mais elle est inexacte. Techniquement parlant, il s'agit d'un droit au déréférencement. La seule question était le traitement des liens hypertextes que l'on retrouve sur Google.

Deuxième élément, nous avons reconnu ce droit au déréférencement à partir du texte de la directive 95/46/CE sur la protection des données personnelles[107] *lu à la lumière des droits fondamentaux. Ce droit n'est donc pas de nature constitutionnelle.*

Troisième élément, il faut savoir que 140 000 demandes de déréférencements ont été déposées en Europe depuis lors et jusqu'à la fin de l'année 2014. C'est un droit qui a donc été fortement utilisé par les citoyens. On ne peut pas dire qu'ils sont inconscients de ce qui se passe, surtout de la part des jeunes qui s'intéressent beaucoup à la protection de leur vie privée.

107 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, constitue le texte de référence, au niveau européen, en matière de protection des données à caractère personnel.

Maintenant, juridiquement, il semble que la stratégie de Google soit d'accepter assez généreusement ces demandes. À ma connaissance, il n'y a pas de litiges jusqu'à présent qui arrivent à la Cour de justice portant sur un éventuel refus de Google à faire droit à une telle demande. Pourquoi ?

Dans la logique de notre arrêt, le droit de l'individu à demander le déréférencement lui accorde la possibilité de le faire directement auprès de Google. Si Google y fait droit, il n'y a plus de différend. Sinon, ce sont les juridictions étatiques qui seront saisies de cette question. Au surplus, la CJUE peut éventuellement trancher sur la base d'une question préjudicielle s'il y a encore des questions relatives notamment à la portée des droits fondamentaux.

Délia Rahal-Löfskog

Concernant les mégadonnées, comme à chaque fois qu'il s'agit de données à caractère personnel, la loi dite « informatique et libertés » trouve à s'appliquer. Par opposition, la loi ne s'applique pas lorsqu'il s'agit de données anonymes.

Une donnée anonyme n'est pas seulement celle expurgée du nom et du prénom. Dans ce cas d'espèce, il s'agirait davantage de données pseudonymisées[108] qui restent donc des données à caractère personnel.

L'utilisation massive des données dans le cadre des mégadonnées suppose une anonymisation préalable pour permettre de ne pas avoir à satisfaire aux principes posés par la loi (finalité, proportionnalité, durée de conservation, sécurité, droits des personnes).

Les données ouvertes (en anglais, « open data ») sont entendues comme la mise à disposition publique des données afin d'être librement réutilisables et suppose l'absence de données personnelles (sauf disposition législative ou réglementaire exprès).

Dès lors qu'il ne s'agit pas de données strictement anonymes, il y a lieu d'évaluer les risques de réidentification des personnes avant de publier les données, en particulier dans le cas de données sensibles. Et dès lors que les informations permettent de remonter à l'individu, un certain nombre de précautions méritent d'être prises. Elles peuvent tout d'abord être de nature technique, comme ne pas permettre l'affichage de résultats en dessous d'un certain seuil. Elles peuvent aussi être de nature juridique en interdisant que le croisement de bases anonymes conduise à la réidentification des personnes.

108 Données protégées par un pseudonyme. Ces données ne sont pas anonymes.





Deuxième table ronde

Quelle régulation des plateformes numériques ?

Le Conseil d'État propose la création d'une nouvelle catégorie juridique de prestataire(s) intermédiaire(s) intitulée « *plateforme* ». 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.

Outre les obligations particulières issues du droit de la concurrence et du droit de la consommation, les plateformes seraient, au titre de l'exigence de loyauté que le Conseil d'État propose, tenues à de nouvelles obligations : pertinence des critères de classement ; obligation d'information, encadrement des retraits de contenus.

La table ronde a pour objet de vérifier la pertinence du concept de « *plateforme* » ainsi défini et des obligations qu'il est proposé de lui rattacher. Ces obligations sont-elles suffisantes au regard de la protection des données personnelles ou, au contraire, excessives au regard de la liberté d'entreprendre et de l'ouverture à l'innovation ?

Des exemples concrets seront pris chez des acteurs tels que les moteurs de recherche, réseaux sociaux, sites de partage de contenus (vidéos, musique, photos, documents, etc.), places de marché, magasins d'applications, comparateurs de prix. Une attention particulière sera consacrée aux contenus audiovisuels et aux services nouveaux proposés aux internautes en matière de logement, de déplacements, de loisirs.

Sommaire





Éléments de réflexion sur la régulation des plateformes numériques

Reconnaissance du rôle de prestataires actifs que sont les plateformes numériques

Le terme de « *plateforme* » est polysémique : une première acception couvrirait notamment les écosystèmes d'applications[109], les sites de partage de contenus et les places de marché, soit tous les sites qui permettent à des tiers de proposer des contenus, des services ou des biens ; une seconde acception, plus large, qui est celle retenue par le rapport du Conseil national du numérique sur la *neutralité des plateformes*[110], couvrirait également tous les sites qui servent de point de passage pour accéder à d'autres contenus, notamment les moteurs de recherche, les agrégateurs ou les comparateurs de prix. Tous ces sites ont en commun d'être des portes d'entrée, soit pour l'expression des internautes, soit pour l'accès des internautes à d'autres biens et services, soit les deux.

Le fait de mettre en avant le rôle joué par les plateformes n'implique pas une dénonciation univoque de ces dernières : les plateformes ont une utilité manifeste tant pour les internautes que pour les offreurs de biens et de services. Il s'agit seulement de constater que ce rôle leur confère un pouvoir et que le pouvoir ne peut pas aller sans responsabilités, sauf à déséquilibrer l'exercice des libertés.

La catégorie actuelle des hébergeurs, définis par leur rôle « *technique et passif* » et leur absence de connaissance et d'intervention sur les informations stockées, ne correspond plus à la réalité des plateformes, qui jouent un rôle actif de présentation, de référencement et de classement. La Cour de cassation a écarté la qualification d'hébergeur pour la société *eBay* et le tribunal de grande instance de Paris a fait de même pour le service de recherche de *Google*. À moyen terme, tous les grands services d'intermédiation utilisés sur Internet pourraient perdre la qualification d'hébergeur et le régime de responsabilité civile et pénale limitée qui en découle. La définition d'une nouvelle catégorie juridique est devenue nécessaire.

Le Conseil d'État propose la création d'une nouvelle catégorie juridique de « *prestataires intermédiaires* » au sens de la directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique, distincte à la fois des éditeurs de contenus et des hébergeurs, et qui serait intitulée *plateforme*.

Seraient ainsi qualifiés 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. Une telle définition couvrirait l'ensemble des acteurs tels que : moteurs de recherche, réseaux sociaux, sites de partage de contenus (vidéos,

109 L'écosystème d'applications recouvre à la fois le support sur lequel les applications peuvent être fournies, l'interface de programmation mise à disposition des tiers pour qu'ils développent leurs applications, et le magasin d'applications.

110 Conseil national du numérique, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014, rapport remis au ministre de l'Économie, du Redressement productif et du Numérique et à la secrétaire d'État chargée du Numérique.

musique, photos, documents, etc.), places de marché, magasins d'applications, agrégateurs de contenus ou comparateurs de prix. Par son caractère générique, elle pourrait également couvrir à l'avenir de nouveaux types de services encore peu développés ou inexistants. Cette définition cherche à cerner 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.

C'est ce rôle d'intermédiaire qui justifie un régime de responsabilité spécifique. En effet, l'article 6 de la loi pour la confiance dans l'économique numérique (LCEN) du 21 juin 2004 distingue les hébergeurs, dont la responsabilité civile et pénale est limitée, des éditeurs, qui sont soumis à un régime de responsabilité similaire à celui de la presse écrite. Cette distinction est aujourd'hui discutée: la jurisprudence a défini l'hébergeur comme l'intermédiaire technique ne jouant pas de rôle actif qui lui permette d'avoir connaissance ou de contrôler les données stockées.

Le cas des moteurs de recherche fait aujourd'hui particulièrement question. Ce ne sont pas des éditeurs de données, mais ils jouent un rôle actif dans le stockage et le référencement de celles-ci en agissant sur leur présentation à l'utilisateur. Saisie sur renvoi préjudiciel de la Cour de cassation de la qualification du service de référencement *AdWords* de *Google*, la Cour de justice de l'Union européenne (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, Gde chambre, aff. C-236/08, 23 mars 2010, *Google France et Google Inc c/ Louis Vuitton Malletier*, paragr. 115)[111]. Le débat judiciaire est toujours en cours : poursuivi sur le terrain de la responsabilité civile par un acteur qui estimait que *Google* était responsable d'un lien référencé par *AdWords* renvoyant à un article mettant en cause sa vie privée, la cour d'appel de Paris, dans un arrêt du 11 décembre 2013, a retenu la qualification d'hébergeur et annulé le jugement du tribunal de grande instance qui s'était prononcé en sens inverse.

S'agissant du service de recherche *naturelle*, le tribunal de grande instance de Paris, dans un jugement du 6 novembre 2013, a écarté la qualification d'hébergeur, retenant, en se fondant sur des documents émanant d'ailleurs de la société *Google* elle-même, l'existence d'un « *choix éditorial* » quant au classement des contenus, la société ayant une entière liberté dans la détermination de son algorithme[112]. L'arrêt *Google Spain* du 13 mai 2014 de la CJUE, s'il porte sur un sujet distinct, celui de la qualification comme responsable de traitement des données personnelles, s'inscrit dans cette tendance à l'affirmation de la responsabilité des moteurs de recherche.

111 À la suite de cet arrêt de la CJUE, la Cour de cassation a cassé l'arrêt de la cour d'appel au motif qu'il n'avait pas retenu les bons critères pour écarter la qualification d'hébergeur et renvoyé l'affaire au fond devant la Cour d'appel de Paris .

112 TGI Paris, 17e ch., 6 novembre 2013, *Mosley c. Google Inc*, n° 11/07970.

Intermédiaire technique, hébergeur, éditeur : rappel des définitions légales

Les catégories dans lesquelles sont couramment rangés les principaux acteurs d'Internet sont définies par la directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique, transposée en France par la LCEN. On distingue :

Les intermédiaires techniques : La qualification d'intermédiaire technique regroupe les trois catégories définies par la section 4 du chapitre II de la directive : les acteurs assurant une prestation de « simple transport », ceux assurant la forme de stockage dite « *caching* » et les hébergeurs. Ces trois catégories ont en commun de ne jouer qu'un rôle « *technique et passif* » dans l'acheminement des informations. Elles bénéficient d'un régime de responsabilité limitée et d'une absence d'obligation générale en matière de surveillance.

Les prestataires de simple transport : L'article 12 de la directive s'applique aux fournisseurs d'accès à Internet et à ceux qui assurent l'interconnexion sans lien direct avec les utilisateurs finaux. Il est transposé en France par l'article L. 32-3-3 du code des postes et des communications électroniques.

Les prestataires de *« caching »* : L'article 13 de la directive définit le « *caching* » comme le « *stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service* ». Il est transposé par l'article L. 32-3-4 du code des postes et des communications électroniques.

Les hébergeurs : L'article 14 de la directive définit l'hébergement comme le service « *consistant à stocker des informations fournies par un destinataire du service* ». Le 2. du II de l'article 6 de la LCEN, un peu plus développé, définit les hébergeurs comme « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ».

Les éditeurs : La directive sur le commerce électronique ne traite pas des éditeurs, sinon en creux : ils ne font pas partie des catégories bénéficiant d'un régime de responsabilité limitée. Le III de l'article 6 de la LCEN les définit comme « *les personnes dont l'activité est d'éditer un service de communication au public en ligne* ». La qualification d'éditeur implique la maîtrise effective du contenu. Les contenus mis en ligne par l'éditeur engagent sa responsabilité civile et pénale.

À moyen terme, tous les grands services d'intermédiation utilisés sur Internet pourraient ainsi perdre la qualification d'hébergeur, avec un impact sur leur régime de responsabilité civile et pénale. En revanche, la catégorie des plateformes n'inclurait pas ceux des acteurs ayant une responsabilité directe dans la mise en ligne des contenus, tels les sites de musique en ligne ou de vidéo à la demande, considérés comme des éditeurs. La définition d'une nouvelle catégorie juridique a donc semblé nécessaire en complément des acteurs habituels.

Respect d'un principe de « loyauté » plutôt que de « neutralité »

Il est parfois proposé d'étendre le principe de neutralité au-delà des seuls opérateurs de communications et de l'appliquer aux plateformes[113]. Les partisans de la neutralité des plateformes soutiennent qu'elles jouent un rôle au moins aussi important que celui des opérateurs de communications dans l'accès des internautes à de nombreux contenus et services. Parmi ces partisans, les opérateurs de communications mettent en avant le partage de la valeur qui s'opère aujourd'hui en faveur des grandes plateformes et à leur détriment ; ils insistent sur le fait que les obligations qui seraient mises à leur charge, en vertu du principe de neutralité des réseaux, devraient être contrebalancées par un principe similaire de neutralité envers les plateformes. Cet aspect n'est pas traité par la proposition de règlement européen, qui ne concerne que les opérateurs de communications.

Les obligations des plateformes ne peuvent pourtant pas être envisagées dans les mêmes termes que celles des fournisseurs d'accès. L'objet de ces plateformes est de fournir un accès organisé, hiérarchisé ou personnalisé aux contenus mis à disposition sur leur site ou auxquels elles donnent accès. En vertu du principe de neutralité de l'Internet, un fournisseur d'accès doit traiter de la même manière tous les sites ; un tel traitement égalitaire ne peut pas 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. Leur liberté éditoriale, consistant à proposer le classement et/ou la présentation qui leur paraissent les plus pertinents, doit être respectée. L'avis du Conseil national du numérique, s'il emploie le terme de *neutralité*, ne préconise pas en réalité d'imposer aux plateformes une obligation d'égal traitement analogue à celle incombant aux opérateurs de communications.

Pour autant, les plateformes sont ou devraient être soumises à plusieurs catégories d'obligations. Le droit actuel les assujettit déjà aux obligations résultant du droit de la concurrence pour les relations des plateformes entre elles et avec les autres entreprises, et du droit de la consommation et du principe de loyauté dont il est porteur pour les relations avec les internautes. L'utilisation qu'elles font des algorithmes justifie que leur soient imposées des obligations spécifiques que le droit actuel ne prévoit pas, ou ne prévoit que de manière incomplète ou insuffisante.

L'étude annuelle 2014 du Conseil d'État propose donc de soumettre cette nouvelle catégorie juridique à une *exigence de loyauté*, tant à l'égard des utilisateurs finals que des tiers qui mettent en ligne leurs contenus ou proposent leurs biens ou leurs services.

Celle-ci consiste à assurer de bonne foi le service de classement ou de référencement proposé, sans chercher à le détourner à des fins contraires à l'intérêt des utilisateurs. La reconnaissance d'un devoir de loyauté pour cette nouvelle catégorie juridique ne

113 V. le rapport 2014 précité du Conseil national du numérique sur la neutralité des plateformes.

change rien aux limites posées à la responsabilité de la plateforme, visant à éviter une trop grande censure sur leurs auteurs. En revanche, elle implique l'émergence d'un nouveau droit spécifique des plateformes.

Déjà soumises à des obligations particulières en droit de la concurrence et en droit de la consommation, les plateformes seraient, au titre de l'exigence de loyauté, tenues à quatre nouvelles obligations (proposition 6) :

- obligation de pertinence des critères de classement et de référencement ;
- obligation d'information sur ces critères ;
- encadrement des retraits de contenus par la plateforme ;
- obligation de notification préalable des changements de politiques relatives aux contenus (pour les utilisateurs commerciaux).

Le Conseil d'État propose par ailleurs, , de développer la participation des utilisateurs des plateformes à l'élaboration des règles éditoriales (proposition 10).





Présentation des intervenants

Président

Christian Paul, *député de la Nièvre, coprésident de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique de l'Assemblée nationale,*

Christian Paul a participé activement depuis plus de quinze ans à tous les débats publics liés à l'Internet (droits d'auteur, lois DAVDSI et HADOPI, régulation, responsabilité, brevetabilité du logiciel, réseaux très haut débit, e-démocratie, etc.). Il a organisé les premières « Rencontres parlementaires pour la société de l'information et de l'Internet » en 1998 à l'Assemblée nationale (retranscrites dans l'ouvrage collectif *La révolution numérique crée-t-elle une révolution juridique ?*). Il est l'auteur du rapport de juin 2000 sur *Les droits et libertés sur l'Internet*, qui a préfiguré la création du Forum des droits sur l'Internet en vue d'une co-régulation de l'Internet. Il est l'auteur d'une proposition de loi sur la neutralité d'Internet (2011). Il co-préside le groupe parlementaire sur l'Internet et la société numérique depuis 2012, et préside l'association « 27e région » pour l'innovation publique. Plusieurs ouvrages rendent compte de ses travaux : *Le défi numérique des territoires* et *Design des politiques publiques*. Il est membre du Conseil national du numérique et du Comité de concertation « France très Haut Débit » (jusqu'en 2014). Il a co-rédigé l'ouvrage programmatique *Vers la cité numérique* (2001) et *La France connectée dans une société créative* (2011). Dans la Nièvre et en Bourgogne, il soutient de longue date la diffusion des usages du numérique.

Intervenants

Nicolas Colin, *inspecteur des finances, entrepreneur*

Nicolas Colin est l'un des associés de la société *TheFamily*, dont il est cofondateur. Diplômé de l'École nationale supérieure des télécommunications de Bretagne et de Sciences Po Paris, ancien élève de ENA, il a été inspecteur des finances de 2006 à 2010 et de 2012 à 2013, ayant fondé et présidé entre-temps une entreprise spécialisée dans le *social marketing*. En 2009 il a été rapporteur, avec Constance Rivière, de la mission « Création et Internet », chargée de formuler des propositions pour le développement de l'offre légale de contenus culturels en ligne. Nicolas Colin est l'auteur, avec Henri Verdier, de *L'Âge de la multitude, Entreprendre et gouverner après la révolution numérique* (Armand Colin, 2e éd. mai 2015) et, avec Pierre Collin, conseiller d'État, d'un rapport d'expertise sur la fiscalité de l'économie numérique remis au Gouvernement en janvier 2013. Il est professeur associé à l'Université de Paris-Dauphine et maître de conférences à Sciences Po Paris. Il est membre de la CNIL depuis février 2014.

Laurent Cytermann, *maître des requêtes au Conseil d'État*

Diplômé de l'École nationale de la statistique et de l'administration économique (ENSAE) en 2001 et de Sciences Po Paris en 2002, ancien élève de l'ENA, Laurent

Cytermann a débuté sa carrière en 2005 comme chef de bureau des minima sociaux et de l'aide sociale à la direction générale de l'action sociale. Il rejoint le Conseil d'État en 2009, où il est chargé des fonctions de maître des requêtes à la section sociale et à la section du contentieux du Conseil d'État ; il est nommé maître des requêtes en avril 2013. Il a exercé de 2012 à 2014 les fonctions de rapporteur général adjoint à la section du rapport et des études et, à ce titre, a notamment co-rédigé l'étude annuelle 2014 sur *Le numérique et les droits fondamentaux*. Il enseigne le droit de la régulation à l'école de droit de Sciences Po Paris.

Francis Donnat, *directeur des relations institutionnelles et des politiques publiques de* Google France

Francis Donnat, diplômé de Sciences Po Paris en 1993, ancien élève de l'ENA (promotion Valmy, 1998), a été auditeur (1998-2001), puis maître des requêtes (depuis 2001) au Conseil d'État. Après avoir été affecté à la section du contentieux puis à la section de l'intérieur, il a été nommé responsable du centre de documentation du Conseil d'État (2002-2004). Il a par la suite exercé les fonctions de commissaire du gouvernement près les formations contentieuses du Conseil d'État (2004-2005) et référendaire à la Cour de justice de l'Union européenne (2005-2012). Francis Donnat a par ailleurs été maître de conférences à l'IEP de Paris (1998-2005) puis professeur associé à l'université de Strasbourg (2009-2012). Depuis le 1er septembre 2012, Francis Donnat est directeur des politiques publiques chez *Google France*. Ses principales publications comprennent *Le contentieux communautaire de l'annulation* (LGDJ, 2008), et *La Cour de justice de l'Union européenne* avec E. von Bardeleben et D. Siritzky (La Documentation française 2012).

Antoinette Rouvroy, *chercheur qualifié au centre de recherche « Information, droit et société », faculté de droit de Namur*

Antoinette Rouvroy, docteur en sciences juridiques de l'Institut universitaire européen, est chercheuse qualifiée du FNRS au centre de Recherche en Information, Droit et Société (CRIDS) à l'université de Namur. La participation à des contrats de recherche européens du CRIDS depuis 2007, puis son mandat de chercheur qualifié du FNRS depuis 2008 ainsi que son mandat d'expert pour le comité de la Prospective de la CNIL française depuis 2012, ont orienté ses recherches vers les enjeux de la gouvernance polycentrique des technologies normatives, et des articulations entre normativités juridique, technologique et sociale. Outre les enjeux du tournant numérique et de ses applications (« *autonomic computing, ambient intelligence, datamining* ») pour les régimes juridiques de protection de la vie privée et des données personnelles, elle développe une nouvelle ligne de recherche, depuis quelques années, autour de ce qu'elle a appelé la « *gouvernementalité algorithmique* ». Auteur de nombreux articles et contributions, elle a dirigé la publication de l'ouvrage intitulé *Law, human agency and autonomic computing : the philosophy of law meets the philosophy of technology* (Routledge, 2011). Elle est aussi l'auteur de *Human Genes and Neoliberal Governance. A Foucauldian Critique*, Routledge-Cavendish, 2008.

Actes – Quelle régulation des plateformes numériques ?

Christian Paul
Député de la Nièvre, coprésident de la commission de réflexion sur le droit et les libertés à l'âge du numérique

La seconde table ronde va nous permettre d'évoquer la régulation des plateformes numériques.

Si ce colloque avait lieu en 2005, il y a fort à parier que la question de la régulation des plateformes n'aurait pas été posée, en tout cas elle ne l'aurait pas été dans les termes que nous employons aujourd'hui. En revanche, si nous étions de nouveau réunis dans dix ans, la question serait sans nul doute encore posée ; non pas que les plateformes ne soient pas mortelles, mais parce que la question est centrale dans le monde numérique. En effet, les grandes plateformes sont les nouveaux empires, comme par exemple les GAFA (*Google*, *Apple*, *Facebook*, *Amazon*) souvent cités. Elles sont à notre époque ce que les grands empires miniers et sidérurgiques furent à la première révolution industrielle. Ce n'est donc pas un hasard si beaucoup de travaux de recherche depuis quelques années, comme l'étude annuelle 2014 du Conseil d'État ou les rapports du Conseil national du Numérique[114], ont mis les projecteurs sur ces acteurs qui jouent désormais un rôle essentiel dans le monde numérique qui est le nôtre.

La Commission numérique et libertés de l'Assemblée nationale, que j'anime avec Christiane Feral-Schuhl, s'en ait également saisi car l'apparition et la puissance des plateformes ne cessent de croître. Leur capitalisation boursière est immense. Leur rôle et leur nature mêmes doivent être décryptés. C'est en quelque sorte un nouveau pouvoir. Je ne sais pas s'il s'agit d'un cinquième ou d'un sixième pouvoir, il y a plusieurs thèses à ce sujet. Mais il s'agit incontestablement d'un nouveau pouvoir par la connaissance intime que détiennent les plateformes de la société et de ses mouvements en profondeur et, surtout, de chacune et chacun d'entre nous. On notera que ce sont avant tout des intermédiaires. Evgeny Morozov, dans sa critique du « *solutionnisme technologique* »[115] parlait même de « *filtres divins* ». Ce sont aussi, Nicolas Colin le dira certainement, des écosystèmes d'innovation d'une ampleur sans précédent.

114 V. notamment les rapports du Conseil national du Numérique, *Citoyens d'une société numérique*, 2013 ; *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014 ; *Jules Ferry 3.0 - Bâtir une école créative et juste dans un monde numérique*, octobre 2014.

115 E. Morozov, *Pour tout résoudre, cliquez ici. L'aberration du solutionnisme technologique*, ed. FYP, 2014 (traduction française de l'ouvrage *To Save Everything, Click Here : Technology, Solutionism, and the Urge to Fix Problems that Don't Exist*, Penguin, 2014).

Un même débat, il y a onze ans, quand nous débattions à l'Assemblée nationale de la loi de confiance dans l'économie numérique[116] (LCEN) de 2004, distinguait simplement les *éditeurs* des *hébergeurs*, avec des régimes de responsabilité différents. Onze ans plus tard, cette table ronde doit éclairer la question désormais fermement posée par l'étude du conseil d'État : « *qu'est-ce qui fonde l'existence même d'une nouvelle catégorie ?* » Quelle est en effet cette nouvelle catégorie d'acteurs qui a émergé il y a une dizaine d'années ? Est-ce une catégorie juridique nouvelle ? Et d'ailleurs faut-il une catégorie juridique nouvelle pour parler de la régulation des plateformes ? Et si oui, quelles seraient, dans ce cas précis, leurs obligations particulières ?

Il est toujours fascinant de voir apparaître un phénomène de cette ampleur. Encore faut-il le définir avec rigueur et sans céder à la séduction. J'ai bien conscience que c'est une question économique, politique, avant d'être un débat juridique. C'est pourquoi les quatre intervenants qui sont à mes côtés apporteront probablement un regard différent et complémentaire sur cette question.

Je vais dans cette introduction vous adresser quelques questions. Quel périmètre ont, au fond, ces grandes plateformes ? Qu'y a-t-il de commun entre un moteur de recherche, une place de marché ou un site d'intermédiation ou de partage ? Il y a évidemment un travail de compréhension. Je demanderai aux intervenants de contribuer à ce travail d'appréhension, de définition et de périmètre. Ce qui est évidemment important pour chacun d'entre nous, dans notre vie quotidienne, c'est que les plateformes sont des portes d'entrée, des points d'accès pour un monde de biens, de services et de contenus, à consulter ou à acquérir. L'intermédiation joue un rôle essentiel, bien sûr dans l'économie depuis toujours, mais il est particulièrement central dans le monde numérique. Les plateformes fournissent des services et permettent également à d'autres acteurs de les enrichir en créant des applications ; j'évoquais toute à l'heure cette idée d'écosystème qui entoure les plateformes et que Nicolas Colin évoquera, mais ces services qui permettent en quelque sorte de définir des plateformes, ce sont d'abord le référencement et le classement. C'est ici que tout commence grâce à la puissance des algorithmes qui utilisent les données personnelles comme un carburant dans un moteur pour classer, créer des profils et répondre à leurs besoins ou sollicitations.

La plateforme agit aussi dans une continuité verticale : jusqu'au terminal, *via* la géolocalisation de votre téléphone mobile ; et jusqu'à produire, le cas échéant, des formats propriétaires dans une intégration économique verticale comme par exemple avec les livres numériques.

Un premier survol, précisé dans l'étude annuelle 2014 du Conseil d'État, fait apparaître plusieurs familles : les sites qui permettent à des tiers de proposer des contenus (biens ou services) et les sites qui servent de point de passage pour accéder à d'autres contenus (moteurs de recherche, agrégateurs et comparateurs de prix).

116 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Si l'on va un peu plus loin que ce travail très rapide de définition, on pourrait avoir une réflexion plus politique relative aux enjeux de régulation. La question posée n'est pas seulement de savoir ce que sont les plateformes, les forces en présence ou les services rendus, mais quels sont les enjeux de cette régulation ? On dit que les plateformes seraient, pour les principales, aussi puissantes que des États. C'est une interrogation démocratique qui vient très vite. Il y a donc bien un mouvement de maîtrise ou de domination, non seulement en raison de la puissance financière actuelle de plusieurs de ces plateformes ou du nombre d'utilisateurs – cette « *multitude* » dont parlent Nicolas Colin et Henri Verdier dans leur livre[117] –, mais également, en raison de la nature des plateformes. Nous y reviendrons avec Antoinette Rouvroy.

Auparavant, les infrastructures essentielles étaient les grands réseaux qui étaient du ressort des États. Aujourd'hui, elles sont fournies par des géants du capitalisme informationnel. Si l'on s'intéresse non pas tant aux milliards de dollars en jeu, mais à la nature même de cette puissance, on observe aussi des influences personnalisées, qui intéressent intimement chacun d'entre nous, alors même que l'on interagit avec des millions d'utilisateurs.

Je mets donc dans le débat cinq enjeux principaux de cette régulation. La question la plus classique est celle de la *responsabilité des plateformes*, qui était posée dès le début des années 2000 avec la directive européenne sur le commerce électronique[118] et la loi française pour la confiance dans l'économie numérique de 2004. Le deuxième enjeu est un enjeu de *concurrence* au sens où l'effet de position dominante des grandes plateformes est aujourd'hui clairement posé ; la Commission européenne l'a posé depuis des années, avec ce droit de vie ou de mort que l'on évoque parfois à propos d'autres acteurs. Le troisième enjeu est amené dans le débat en particulier par un rapport du Sénat de 2014 qui évoquait justement les *infrastructures essentielles* gérées par des entreprises privées[119]. La question qui était posée par le Sénat, qui s'interrogeait sur la régulation des plateformes, non plus seulement par le droit de la concurrence mais par cette idée d'infrastructures essentielles, c'était de dire que l'exercice de certaines activités économiques devient impossible sans le recours à la facilité que représentent les plateformes ; ce qui peut constituer un frein à l'innovation mais aussi menacer le pluralisme. Le quatrième enjeu est la *protection de la vie privée et des données personnelles*, sujet qui a été abordé par la table ronde précédente, avec les questions de catégorisation des profils et tout ce qui relève de près ou de loin d'une société de surveillance – nous avons vu à la faveur de l'affaire Snowden comment les grandes plateformes étaient invitées à coopérer avec les États dans leur mission régalienne –. Je le dis avec beaucoup de diplomatie pour préserver les relations transatlantiques. Le cinquième enjeu est, pour reprendre les termes de

117 N. Colin et H. Verdier, *L'Age de la multitude - Entreprendre et gouverner après la révolution numérique*, ed. Armand Colin, 2012.

118 Directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique dans le marché intérieur, dite « *directive sur le commerce électronique* ».

119 Sénat, rapport d'information n° 696 du 8 juillet 2014, *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*.

Mme Rouvroy, la « *nouvelle rationalité algorithmique* », qui concerne les effets des plateformes sur les décisions individuelles et collectives avec une personnalisation, sans qu'il y ait forcément une maîtrise par les individus de cette personnalisation. Ce sont des enjeux de démocratie. Une question de régulation est toujours une question où la démocratie tente de projeter ses propres valeurs. Il y a un risque de censure algorithmique, je crois qu'Evgeny Morozov parle du « *péril de la surveillance algorithmique* ». Ce cinquième enjeu est un enjeu de dessaisissement de la décision individuelle ou collective et il est, à mes yeux, essentiel.

Nous évoquerons ensuite la problématique de l'identification des règles. Le travail collectif des juristes, des experts, de la société civile et des chercheurs est d'essayer dans un mouvement de réflexion collectif, en France et en en Europe, d'imaginer les règles pour protéger nos droits fondamentaux. Un nouveau régime de responsabilité est en débat. Les plateformes perdront probablement progressivement, du moins en partie, le régime de responsabilité limitée de la loi pour la confiance dans l'économie numérique. Il leur faudra trouver les voies d'une responsabilité aménagée (les hébergeurs étaient passifs à l'origine et leur responsabilité limitée) pour les mettre à l'abri du fait d'un tiers, car les plateformes ont développé des métiers et leur référencement n'est plus passif, il est même terriblement actif. À l'inverse, dans un certain nombre de cas, la responsabilité de la plateforme sur le contenu peut rester limitée y compris pour éviter qu'elle ne censure elle-même du contenu. Il faudra trouver des points d'équilibre. Il y a un deuxième type d'obligations qui relèvent déjà du droit de la consommation et de la concurrence (abus de position dominante), les obligations particulières qu'un acteur doit supporter alors qu'il occupe 80 ou 90 % du marché. Faut-il aller jusqu'à la désintégration verticale comme il a déjà été procédé dans d'autres domaines du droit de la concurrence ?

Enfin, les plateformes pourraient dans l'avenir, et c'est l'une des questions essentielles posées par le Conseil d'État, être tenues à de nouvelles obligations au titre d'un principe nouveau : « *l'exigence de loyauté* ».

Je préfère cette notion à l'idée de neutralité qui a été utilisée par le Conseil national du numérique, car il est difficile d'envisager la neutralité d'une plateforme y compris lorsqu'on lui demande un service qui n'est pas d'être neutre à proprement parler. En revanche, nous pouvons exiger qu'elle soit loyale. Je ne dis pas que cela suffise, mais cela peut être un principe qui permette de construire progressivement une régulation en s'interrogeant et en fixant des règles sur la pertinence des critères de classement, sur l'obligation d'information et sur l'encadrement des retraits de contenu. Ces obligations sont-elles suffisantes au regard de la protection des données personnelles ou, au contraire, excessives au regard de la liberté d'entreprendre et de l'ouverture à l'innovation ? Comment encadrer les algorithmes prédictifs ? Est-ce qu'un jour le juge ira à l'intérieur de la machine elle-même ? L'apparition sur une décennie d'acteurs majeurs, un besoin de règles nouvelles, des principes tout juste émergents, voilà le menu de cette table ronde.

Nicolas Colin
Inspecteur des finances, entrepreneur

Je souhaiterais dire quelques mots sur l'émergence de cette réalité industrielle que l'étude du Conseil d'État désigne sous l'appellation de « *plateforme* ». Au début du développement de l'économie numérique, au milieu des années 1990, les plateformes n'étaient pas des entités clairement définies, que ce soit pour les observateurs ou pour les premiers acteurs de cette économie. Nous étions familiarisés avec les effets de concentration observés sur les marchés tels que celui des systèmes d'exploitation avec les grands cas *anti-trust* contre l'entreprise *Microsoft* à cette époque-là. Mais, à vrai dire, quand Internet a commencé à se développer, il a été appréhendé avant tout comme un nouveau canal de communication. C'est que l'on a appelé l'ère du « *Web 1.0* » : un certain nombre d'acteurs traditionnels, producteurs de contenu ou vendeurs de produits, ont considéré qu'Internet était un nouveau canal de communication, de prescription, de marketing ou de distribution qui leur permettrait de rassembler les anciens clients et d'en toucher de nouveaux. Ainsi, Internet a d'abord été inscrit dans le paradigme d'un monde dominé par les économies d'échelle, où les acteurs les plus gros ont une taille critique qui leur permet de dicter leurs conditions au marché et de s'imposer face à leurs concurrents. Un élément classique de cela, c'est le marché audiovisuel entre les chaînes de télévision hertzienne. On sait très bien qu'il y a une prime importante à celles qui font régulièrement les plus gros scores d'audience : cela leur permet de facturer plus cher leurs espaces publicitaires, ce qui accroît leurs revenus et leur permet de financer des programmes nouveaux, etc. Ce sont donc les économies d'échelle, liées à la taille de l'audience, qui donnent un avantage à une entreprise par rapport à ses concurrents. Internet a donc été abordé d'abord comme un acteur de réplication de cet univers. Plutôt que de diffuser par les ondes hertziennes, on allait diffuser par le fil téléphonique, vecteur de ce « *réseau des réseaux* » qu'on apprenait tout juste à maîtriser.

Ce n'est que quelques années plus tard que l'on a commencé à découvrir une nouvelle réalité, une nouvelle particularité d'Internet qui le différenciait radicalement des canaux traditionnels de communication et de distribution : *la puissance des interactions horizontales*. Ce malentendu initial n'est pas surprenant : à chaque fois qu'une nouvelle technologie ou un nouveau média apparaît, les historiens de la technologie nous montrent qu'on commence toujours par employer la nouvelle technologie pour faire ce que l'on faisait déjà avec les anciennes technologies. Par exemple, quand le téléphone est apparu, on a commencé par l'utiliser pour faire ce que l'on faisait déjà avec le télégramme, c'est-à-dire échanger quelques brèves informations et raccrocher aussitôt. Ce n'est qu'avec un peu de pratique que l'on s'est aperçu de la possibilité d'avoir des conversations beaucoup plus longues et du fait que cela changeait radicalement la nature de la communication. Ce n'est donc pas étonnant que l'on se soit mépris, au début, sur Internet.

La prise de conscience de la spécificité d'Internet s'est manifestée de façon assez éloquente, en 1999, par un opuscule intitulé *The Cluetrain Manifesto*[120] rédigé par quatre auteurs voulant défendre la nature horizontale et l'importance du

120 *The Cluetrain Manifesto : The End of Business as Usual*, Levine, Locke, Searls et Weinberger, 1999.

pair à pair (« *peer to peer* ») dans l'expérience numérique. Ils l'ont formulé de façon assez provocante notamment pour les entreprises en leur disant : « *depuis plusieurs années, vous considérez qu'Internet est un canal de communication descendant,* « top-down ». *Vous commencez à peine à vous en emparer, mais les individus ne vous ont pas attendus : ils ont déjà nourri entre eux des conversations vives et spontanées, dynamiques, de sorte qu'au moment où vous arrivez vous apparaissez comme des intrus. Vous voulez utiliser [Internet] comme un canal de communication descendant, mais les individus se sont déjà emparés d'Internet pour nourrir des interactions horizontales, des interactions entre eux, à une échelle et avec une puissance sans précédent dans l'histoire économique et industrielle* ».

Cela change la réalité de toutes les organisations humaines, car dans l'univers numérique on peut interagir, laisser des traces ; il se noue entre les individus eux-mêmes des interactions qui créent de la valeur et génèrent des réalités nouvelles appelées *effets de réseau*, inexistantes dans la plupart des modèles d'affaires traditionnelles. Pour les téléspectateurs d'une chaîne de télévision, par exemple, ceux-ci sont tous rivés devant leurs écrans, et c'est simplement la masse de cette audience qui donnait à la chaîne un avantage concurrentiel : il y a économies d'échelle mais pas d'effets de réseau directs entre les utilisateurs. À l'opposé, sur Internet, des liens se construisent entre tous ceux qui utilisent la même application ; ils ne sont plus passifs mais actifs. Ils communiquent entre eux. Ces interactions créent de la valeur et rendent plus attractives les applications qui ont le plus d'utilisateurs.

Pour illustrer cela, je prendrai l'exemple de la société *Amazon*. Lorsque vous discutez avec des grands distributeurs, la plupart d'entre eux relativisent la création de valeur dans le monde numérique en disant : « *Finalement Amazon fait le même travail que moi : son cœur de métier est celui d'un grand distributeur ; il a une capacité à négocier avec d'autres fournisseurs et dispose d'une immense infrastructure logistique qui lui permet d'acheminer des produits, depuis les entrepôts où ils sont stockés jusqu'aux clients qui souhaitent en faire l'achat* ». De ce point de vue-là, c'est rassurant pour les grands distributeurs parce qu'ils se disent qu'*Amazon* est comme eux, soumis à la loi des rendements décroissants qui implique que « *plus c'est grand, plus c'est difficile* » et « *plus on a de clients, plus il est difficile de conquérir* un *client supplémentaire* ». Pourquoi ? Car avec une telle échelle d'opérations, l'infrastructure logistique est de plus en plus difficile à optimiser. Au bout d'un moment on s'essouffle, et cela explique que, sur la plupart des marchés traditionnels soumis à la loi des rendements décroissants, où il n'y a pas d'effets de réseau, les entreprises se partagent un marché avec des parts qui sont à peu près fixes : l'une domine avec 40 %, une autre suit avec 25 ou 30 %, puis deux ou trois autres sociétés se partagent le reste du marché et enfin 10 à 15 % du marché est réparti entre des acteurs de niche. C'est ce que nous rappellent les grands distributeurs quand ils se rassurent à bon compte, en considérant *Amazon* de cette manière-là.

Mais dans le modèle d'affaire d'*Amazon* il n'y a pas que l'aspect logistique, il y a aussi le versant numérique grâce auquel *Amazon* noue des liens directement avec ses clients à travers ses applications. Sur le versant numérique sont déployées un certain nombre de fonctionnalités qui, prises isolement, n'ont l'air de rien mais qui,

mises ensemble, combinées les unes avec les autres, génèrent des interactions entre les utilisateurs et exercent des *effets de réseau* qui rendent l'activité d'*Amazon*, non pas à rendement décroissant, comme une infrastructure logistique, mais à rendement croissant !

Ces interactions sont de différentes natures. Par exemple, sur *Amazon*, vous pouvez déposer des avis sur les produits ; le client suivant, qui vient après vous, va pouvoir consulter l'avis que vous avez déposé ; on voit pourquoi cela exerce des effets de réseau : plus il y a de clients, plus il y a d'avis ; plus les avis qui vont être sélectionnés vont être pertinents et représentatifs, plus le client marginal (celui qui arrive, qui est nouveau), va trouver une utilité à rejoindre *Amazon* plutôt qu'un autre vendeur de détail en ligne. Un autre exemple, ce sont les algorithmes de recommandation. Tout le monde sait qu'un algorithme n'a aucune valeur s'il n'est pas nourri et entraîné par de très nombreuses données. Parce qu'*Amazon* a beaucoup de clients, ses algorithmes sont les mieux entraînés du marché et donc les plus pertinents en termes de résultat. C'est plus intéressant de se faire recommander quelque chose par l'algorithme d'*Amazon* que par l'algorithme de la *Fnac* par exemple, parce que la *Fnac* a moins de clients. Cela renverse la logique industrielle. Tout d'un coup, plus on a de clients, plus c'est facile d'en avoir des supplémentaires alors que dans le monde traditionnel, plus on a de clients, plus il est difficile d'acquérir un client supplémentaire.

Le devenir d'un marché où dominent les rendements croissants, c'est que, tôt ou tard, un seul acteur va dominer l'ensemble du marché : on parle de *monopole naturel*. C'est ce qui se passe dans les activités de réseaux traditionnels (télécommunications, transport ferroviaire, etc.). Tôt ou tard, un réseau qui devient plus puissant que les autres sort du lot, souvent pour des raisons un peu contingentes. Mais, parce qu'il sort du lot, il a, à un moment donné, plus de clients que ses concurrents et, par conséquent, les clients marginaux qui arrivent sur ce marché n'ont aucun intérêt à rejoindre le deuxième ou le troisième ; ils ont toujours intérêt à rejoindre le *leader* du marché parce que c'est lui qui crée le plus de valeur pour ses clients.

Amazon a su, fonctionnalité par fonctionnalité, déployer ses effets de réseau pour déjouer la malédiction des rendements décroissants. Aujourd'hui, *Amazon* est globalement à rendement croissant. Grâce au rendement croissant généré sur le versant numérique, *Amazon* n'est pas emportée par le fond, par la taille extraordinaire de son infrastructure logistique. C'est un peu par hasard, en mettant bout à bout toutes ces fonctionnalités, que ses dirigeants se sont aperçus que cela générait ces puissants effets de réseau, qui ont fait d'*Amazon* ont une très grande entreprise du numérique.

Aujourd'hui ce modèle où prédominent les interactions entre pairs est beaucoup mieux compris. On a même mis un mot dessus : le « *Web 2.0* », c'est-à-dire l'Internet dominé par les interactions horizontales entre les utilisateurs d'une même application ou les développeurs qui utilisent les mêmes ressources logicielles. Le « *Web 2.0* » est aujourd'hui maîtrisé, compris par une immense communauté d'entrepreneurs, d'investisseurs, d'observateurs, d'auteurs, d'économistes – à tel point qu'il est devenu vain de lancer une nouvelle activité dans l'économie

numérique sans immédiatement chercher à faire levier des interactions qui vont se nouer entre les utilisateurs d'une même application et/ou les développeurs utilisant la même plateforme logicielle –. Pour cette raison, on a ce surgissement du modèle des *plateformes*, cette bataille industrielle permanente entre ceux qui cherchent à prendre ces places dominantes, à capter la puissance des effets de réseau et à installer leur entreprise dans une position dominante sur tel ou tel marché.

Pour finir, il y a finalement deux grandes catégories de filières. Personnellement, je découpe l'économie en filières : automobile, banque, transports, bâtiment, énergie, etc. Dans certaines filières, la transition numérique est déjà achevée, ou presque, et en général une entreprise domine grâce à la plateforme sur laquelle la filière continue de soutenir son effort d'innovation. *Google* et *Facebook* sont les grandes plateformes de la filière publicitaire. *Amazon* est la plateforme de la filière du livre. Au final, il est très difficile de remettre en cause leur position parce que ces entreprises réussissent à maintenir leur effort d'innovation, à diversifier leurs produits et à s'allier solidement avec leurs utilisateurs. Certes, cela peut empêcher l'innovation et les opportunités pour de nouveaux entrants. Mais en réalité ces derniers, au lieu d'aller concurrencer l'entreprise en place, se posent sur sa plateforme et s'emparent de ses ressources pour affiner ou développer de nouvelles applications. On a tous cette expérience quotidienne lorsque l'on utilise les applications de nos téléphones mobiles : ces applications sont développées par des entreprises qui s'emparent des ressources mises à disposition par des plateformes pour créer de nouvelles applications.

En revanche, dans d'autres filières la course n'est pas encore gagnée, et l'on voit la bataille très rude que se livrent les différentes entreprises pour déterminer qui déploiera la plateforme qui portera telle ou telle filière après sa transition numérique.

L'une des batailles les plus ardentes en ce moment a lieu dans le transport individuel, avec une entreprise qui sort du lot de façon assez spectaculaire, en exerçant de très puissants effets de réseau : *Uber*. Celle-ci a dévoilé il y a quelques semaines des chiffres spectaculaires sur l'élargissement du marché du transport individuel à San Francisco. Ce marché, avant l'arrivée d'*Uber*, était selon elle de 140 millions de dollars par an aux mains des taxis. Aujourd'hui, à San Francisco, *Uber* génère à elle seule 500 millions de dollars de volume d'affaires par an sur le marché du transport individuel. C'est dire la puissance de la plateforme déployée, et la puissance des effets de réseau qu'ils ont su créer du côté des chauffeurs et des clients. Avec cet exemple, on comprend mieux comment une plateforme émerge dans l'économie numérique pour s'installer naturellement dans l'économie réelle, avec des effets de réseau dont le résultat tend à conduire à la constitution d'un monopole naturel (*cf*. le secteur des télécoms).

La nuance ici est que les effets de réseau dans l'économie numérique ne sont pas ceux des grandes infrastructures matérielles traditionnelles (par exemple, réseau de télécommunications ou de transport). Autrement dit, les positions dominantes qui s'installent grâce aux effets de réseau sont en réalité beaucoup moins solides

qu'elles ne l'étaient dans le monde industriel. Ces effets de réseau numériques sont appelés par les économistes spécialisés « *the demand-side network effects* », c'est-à-dire des effets de réseau qui s'exercent du côté de la demande (et non pas du côté de l'offre).

Les réseaux cristallisent la position dominante d'une plateforme. Ce ne sont pas les points d'une infrastructure matérielle telle qu'un réseau de télécommunications ou de transport ferroviaire, mais des liens virtuels noués entre utilisateurs. Ces réseaux sont beaucoup plus immatériels et peuvent s'effondrer quasiment du jour au lendemain si les utilisateurs décident de cesser d'interagir ou d'utiliser leurs services. En ce cas, l'effet de réseau s'estompe d'un seul coup et la multitude déserte en masse une plateforme pour aller vers une autre. Cela s'est déjà vu dans l'histoire de l'économie numérique.

Ensuite, une pression constante est maintenue sur les plateformes. Même gérant l'infrastructure de toute une filière, elles sont systématiquement aiguillonnées, remises en cause, menacées par l'arrivée incessante de nouvelles jeunes pousses sur le marché[121]. Cela n'effraie pas les entrepreneurs de s'attaquer au monopole d'une plateforme, et certains portent de rudes coups aux positions établies des grandes entreprises numériques. D'ailleurs, les plus grandes entreprises numériques sont assimilées parfois à un cartel qui se réunirait régulièrement et secrètement pour se partager le monde numérique au détriment des utilisateurs, à l'instar de l'OPEP pour le pétrole. La réalité, c'est que ces entreprises sont déjà en guerre les unes contre les autres, et qu'elles sont prêtes à s'emparer du marché des autres entreprises si l'une d'elles trébuche. Une action facilitée, notamment, par la porosité du monde numérique entre les différentes filières, les faibles barrières à l'entrée et la fluidité de l'information.

Le dernier point que je voudrais aborder pour nuancer le caractère prétendument inexpugnable des positions dominantes acquises par ces plateformes, c'est la difficulté à qualifier leurs activités.

Dans le monde industriel antérieur, on voyait émerger un usage qui était celui de parler au téléphone, lié à une infrastructure qui permettait de faire cela. On pouvait le codifier dans des règles juridiques et le soumettre à un régime de régulation sous la surveillance d'une autorité administrative telle que la FCC[122] aux États-Unis ou l'ARCEP[123] en France. Dans l'économie numérique, il est beaucoup plus difficile de cerner et de figer un usage ainsi que la nature d'un service rendu. Pourtant d'aucuns prétendent que les choses sont simples : la recherche, c'est sur *Google* ; les interactions entre amis sur *Facebook* ; et l'achat de produits en ligne sur *Amazon*. Ce faisant, ils divisent l'économie numérique en trois. Mais, en réalité, si l'on y regarde de plus près, tout ce qui est service évolue en permanence et les activités s'interpénètrent et évoluent au gré de synergies avec d'autres produits ou services. Ces services sont transformés par les utilisateurs eux-mêmes, affinés par des développeurs qui créent des applications spécialisées sur les plateformes,

121 Jeune pousse ou entreprise innovante en forte croissance (en anglais, « *Start-up* »).
122 *Federal Communications Commission*.
123 Autorité de régulation des communications et des postes.

et il est donc très difficile de mettre en place une régulation sectorielle dans l'économie numérique parce que l'on va s'attacher à un état des choses qui sera périmé à brève échéance. L'un des exemples est la difficulté que rencontre *Google* sur le marché publicitaire des téléphones mobiles : si *Google* domine le marché publicitaire en ligne sur ordinateur (et navigateur), l'entreprise a, en revanche, beaucoup plus de mal à valoriser l'espace publicitaire sur le téléphone parce que l'usage des utilisateurs de téléphone mobile contourne le moteur de recherche et remet en cause sa position dominante sur le marché numérique de la publicité. Il est donc très difficile pour un régulateur d'objectiver ou de qualifier dans la loi la nature d'un service pour le soumettre à régulation ou pour apprécier un marché pertinent, comme on le fait traditionnellement en politique de la concurrence.

Christian Paul
Député de la Nièvre, coprésident de la commission de réflexion sur le droit et les libertés à l'âge du numérique

Le défi est donc directement adressé à Laurent Cytermann.

Laurent Cytermann
Maître des requêtes au Conseil d'État

Je vais essayer de vous expliquer pourquoi le Conseil d'État a proposé la création d'une nouvelle catégorie juridique, celle des *plateformes*, et pourquoi il a proposé d'appliquer à ces prestataires un *principe de loyauté*. Cette notion n'a pas été créée *ex nihilo*. Elle était dans l'air du temps, a mûri avec l'évolution du monde numérique, notamment à travers les réflexions de Nicolas Colin et Henri Verdier sur la notion de plateforme. L'idée de créer une nouvelle catégorie juridique n'était pas évidente et la nécessité ne nous est apparue que chemin faisant, pendant notre réflexion.

Le point de départ, vous l'avez déjà évoqué M. le député et Nicolas Colin, c'est que sur Internet il y a une surabondance d'offres accessibles aux utilisateurs, qu'il s'agisse d'offres de contenu culturel ou informationnel, de biens ou de services, et cela crée un besoin du public d'avoir des intermédiaires, des portes d'entrée pour s'orienter dans cette offre surabondante. Il y a un besoin *d'intermédiation* qui se fait jour, voire de « *réintermédiation* ». D'ailleurs, le rapport qui est sorti récemment de Philippe Lemoine sur *La transformation numérique de l'économie,* en fait une des règles de ce qu'il appelle « *la grammaire du numérique* » ; c'est une expression qui montre bien la nécessité de cette intermédiation.

On arrive donc sur des réalités qui sont en apparence diverses mais, pour nous, ces sociétés ont en commun d'avoir su développer des services de classement ou de référencement de contenus de biens ou de services édités ou produits par d'autres et partagés sur leurs sites. Les exemples sont multiples : magasins d'applications pour téléphones mobiles, places de marché, sites de partage de contenus (vidéos, photos, etc.). Il existe aussi d'autres types de plateformes que sont les moteurs de recherche, les comparateurs de prix ou les agrégateurs d'informations. Certes, ce

n'est pas sur le moteur de recherche qu'on propose l'information, mais le moteur de recherche rend accessible l'information qui est éditée par d'autres sites et par conséquent sert de point d'entrée.

Tous ces exemples ont été abordés dans l'étude annuelle 2014 du Conseil d'État. D'autres domaines encore auraient pu être cités, témoignant de l'omniprésence de cette réalité : dans le domaine du jeu vidéo avec la plateforme *Steam* qui, en l'espace de quelques années, a acquis une position dominante, mais aussi dans le domaine de l'édition scientifique avec la plateforme *Elsevier* qui est devenue incontournable pour la publication et l'accès à la recherche, ce qui peut d'ailleurs poser problèmes aux organismes publics de recherche parce qu'il y a une captation de la valeur de la recherche publique par cette plateforme.

Cette dimension de *porte d'entrée* des plateformes leur donne un double pouvoir : un pouvoir économique avec une captation de la valeur grâce – comme l'a souligné Nicolas Colin – à la relation directe qu'elle noue avec les utilisateurs et qui leur permet de collecter leurs données, et un pouvoir de prescription, d'influence culturelle ou idéologique. Une affaire récente l'illustre particulièrement : le groupe de presse allemand *Axel Springer* avait essayé d'interdire à *Google* de publier le résumé de ses articles de journaux et y a renoncé très rapidement, en novembre 2014, parce que la chute de fréquentation de son site était trop importante. Cela montre à quel point ces plateformes sont devenues incontournables.

Pourquoi les régimes juridiques actuels ne sont pas, selon l'étude du Conseil d'État, satisfaisants pour traiter cette réalité ? Je vais me centrer sur la question de la *responsabilité* avec les distinctions éditeur-hébergeur ; sachant qu'il y a d'autres questions qui se posent sur le plan du droit de la concurrence ou de la diversité culturelle.

La dualité éditeur-hébergeur est issue de la loi pour la confiance dans l'économie numérique de 2004 qui transpose la directive « *commerce électronique* » de 2000. Le mot *hébergeur* désigne les personnes qui mettent à la disposition du public, *via* des services de communication publics en ligne, le stockage des signaux, sons et images fournis par les destinataires du service. La directive précise que cette activité a un caractère purement technique, automatique et passif et qu'il ne faut pas que les hébergeurs aient de connaissance ni de contrôle des informations qu'ils stockent. C'est à ces conditions que les hébergeurs bénéficient d'une responsabilité civile et pénale limitée : si les services qui sont rendus accessibles par l'hébergeur enfreignent la loi, l'hébergeur n'en sera pas responsable sauf si cela lui a été signalé ou s'il est démontré qu'il a eu une connaissance de cette illicéité. Ce régime est vu, à juste titre, comme protecteur de la liberté d'expression et de la liberté d'entreprendre parce que cela évite que les hébergeurs ne soient tentés d'imposer des filtrages pour se prémunir de l'engagement de leur responsabilité.

Pour les plateformes, il est important de bénéficier de la qualification d'hébergeur pour limiter leur responsabilité. Néanmoins, des évolutions de la jurisprudence montrent que leur inscription dans cette qualification d'hébergeur conçue avant leur apparition est fragile. Il existe en ce sens de la jurisprudence de la Cour de justice de l'Union européenne (CJUE) et de la Cour de cassation de 2012 sur les

places de marché, notamment sur *eBay*. La CJUE souligne que l'assistance fournie par la plateforme consistant à optimiser la présentation des offres, si elle existe, fait que l'on n'est plus considéré comme hébergeur. Il y a également un arrêt de la cour européenne sur les services de recherche sponsorisée *AdWords* de *Google*. On a aussi, même si c'est d'un niveau moindre, un jugement du tribunal de grande instance (TGI) de Paris dans l'affaire *Mosley*[124] sur les services du moteur de recherche de *Google* qui refuse la qualification d'hébergeur à ce service. Certes, la jurisprudence est encore en mouvement. Par exemple, sur *Youtube*, il y a parfois des décisions de la justice française et américaine qui maintiennent la qualification d'hébergeur mais avec un argumentaire qui est intéressant pour le débat : le TGI de Paris qui s'est fondé sur le fait que *Youtube* dont vous voyez bien, si vous l'utilisez, qu'il optimise sa page de présentation pour vous, juge que cette optimisation qui résulte de statistiques et d'algorithmes est automatique. Pour le TGI de Paris, cela ne permet pas de caractériser une connaissance de l'information stockée parce que c'est un algorithme. Mais cela entre en tension avec d'autres tendances de la jurisprudence, comme par exemple l'arrêt *Google Spain* de la CJUE[125] qui ne s'est pas du tout arrêté au fait que *Google* scannait automatiquement toutes les informations qui étaient sur Internet pour lui dénier la qualité de responsable de traitement. Le fait qu'on ait des algorithmes, pour dire les choses simplement, n'empêche pas qu'on soit responsable. On a donc cette tendance de la jurisprudence à la fragilisation de la qualification d'hébergeur pour les plateformes et, même si ce n'est pas totalement définitif, cette incertitude est un problème par elle-même.

La position du Conseil d'État dans son étude annuelle 2014 est que cette fragilisation est dangereuse, parce que ce régime des hébergeurs est protecteur de la liberté d'expression et de la liberté d'entreprendre. On ne propose pas– et cela n'est pas toujours bien compris dans le débat –que sur le plan de la responsabilité des contenus, les plateformes soient plus responsables que ne le sont les hébergeurs aujourd'hui. Ce que l'on dit, c'est qu'il faut garder ce régime de responsabilité limitée parce qu'il est protecteur des libertés, en le rebâtissant sur un autre fondement qui n'est pas le caractère purement technique et passif, mais qui est le fait que les contenus rendus accessibles par la plateforme ne sont pas produits ou édités par elle, car son rôle est seulement de les rendre accessibles. Il n'y a donc aucune raison qu'elle en soit tenue pour responsable au même titre que l'éditeur. Par contre, là où la plateforme peut être tenue pour responsable, c'est pour son service de classement et de référencement où elle joue un rôle actif, et pour lequel on propose d'appliquer un principe de loyauté.

Le Conseil propose de privilégier la notion de *loyauté* des plateformes, et non de neutralité comme pour les opérateurs de communications électroniques qui en principe doivent traiter toutes les communications de manière identique. La plateforme, par essence, propose un service de classement ; il n'y a donc pas de raison de lui demander de traiter tout le monde à l'identique. Par contre, on peut attendre d'elle qu'elle soit loyale dans ce service. La définition que l'on donne de la loyauté est qu'elle assure de bonne foi le service de classement et de

124 TGI Paris, 17e ch., 6 novembre 2013, RG 11/07970, *Max Mosley c. Google Inc et Google France*.
125 CJUE, aff. C-131/12, 13 mai 2014, *Google Spain et Google*.

référencement, sans chercher à l'altérer ou le détourner à des fins étrangères à l'intérêt des utilisateurs, par exemple en le présentant sous des aspects objectifs alors qu'il résulterait en partie de partenariats noués entre la plateforme et les services qu'elle référence. Dans ce cas précis, il faudrait au moins être transparent sur ces liens partenariaux.

Le Conseil a proposé de décliner ce principe général de loyauté en différentes obligations spécifiques parce que les plateformes opèrent sur des marchés « bifaces » avec, d'un côté, les utilisateurs et, de l'autre, le contenu des produits qui sont rendus accessibles par la plateforme. Le principe de loyauté s'applique sur ces deux éléments. Il y a des obligations de pertinence du service de classement au regard d l'intérêt des utilisateurs, et de transparence sur les critères de classement. Il y a également des obligations qui concernent les retraits de contenu puisque, souvent, les plateformes ont des politiques sur ces contenus dont elles autorisent ou pas la publication sur leur site. Il faut que les critères de ces politiques soient transparents, non discriminatoires et, surtout, qu'il y ait en cas de désaccord un échange contradictoire avant leur retrait. Concernant les utilisateurs professionnels, les changements d'algorithmes que font régulièrement les plateformes peuvent amener un acteur économique à voir brusquement son rang de classement se dégrader dans la sélection, jusqu'à menacer parfois sa survie économique. Ce pouvoir de prescription de la plateforme crée une responsabilité qui pourrait se traduire, par exemple, par une obligation de notification préalable des changements d'algorithmes dans un certain délai.

Pour conclure, je voudrais souligner que ces distinctions entre éditeur et hébergeur relèvent du droit de l'Union européenne. On ne peut donc pas la surmonter sans modifier le droit de l'Union et notamment la directive sur le commerce électronique. Actuellement, il n'y a pas de projet de réforme en cours de cette directive, mais plusieurs acteurs en France ont fait remarquer qu'il y a un projet de réforme en cours sur la directive dite « *des droits d'auteur* »[126] ; or les deux sujets étant assez liés, ils ont demandé qu'ils soient ouverts conjointement. Ces réflexions peuvent trouver des prolongements dans ces évolutions européennes.

Antoinette Rouvroy
Chercheuse qualifiée au centre de recherche en information, droit et société de la faculté de droit de Namur

J'ai une question qui tient à l'étonnement qui est le mien concernant la confiance que gardent les internautes envers ces services, fournis par des acteurs à la fois connus et inconnus (les nouveaux entrants). La question que je me pose est relative à la nature et aux conditions de la confiance de ceux que l'on appelle les *utilisateurs* dans l'économie numérique. La confiance n'est pas seulement « *un phénomène cognitif reposant sur l'évaluation rationnelle de la fiabilité* » du partenaire ou du confident, comme le voudraient certains théoriciens du choix rationnel, mais un phénomène « *irréductible à une conceptualisation de la rationalité utilitariste,*

126 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.

individuelle, intéressée et optimisatrice »[127]. Il existe différents types de confiance. On peut ainsi évoquer la confiance *routinière* que les individus peuvent développer par rapport à des personnes avec qui ils ont l'habitude d'interagir (médecin de famille, etc.) ; la confiance assurée par la possibilité, si le partenaire ne remplit pas ses engagements, d'aller en justice obtenir l'exécution forcée d'un contrat, par exemple, ou la prise en charge, par des institutions d'assurance, des préjudices éventuels générés par les manquements du partenaire ; la confiance décidée qui est une confiance accordée sans raison, un saut dans l'incertitude radicale, assumé comme tel, et dont on pourrait penser qu'elle est la seule vraie confiance qui vaille puisque c'est celle par laquelle justement on prend consciemment un risque. Ces trois types de confiance (il y en a d'autres), ne sont pas exclusives les unes des autres, et, dans une situation donnée, la routine, l'assurance et la décision se combinent en proportions variables pour contribuer à faire émerger la confiance[128].

Mais la question qui se pose dans le contexte qui nous intéresse est la suivante : comment se forme la confiance des internautes relativement aux acteurs de l'Internet que sont les plateformes, et, en particulier, relativement aux nouveaux entrants (nouvelles plateformes) ? De quelle combinaison de routine, d'assurance et de décision dépend l'émergence de la confiance à l'égard d'acteurs de plus en plus nombreux, offrant des services de plus en plus diversifiés, interagissant avec les utilisateurs sur un mode à la fois automatique et personnalisé ? En réalité, je pense que ces plateformes ont une certaine capacité à produire elles-mêmes l'adhésion potentielle des utilisateurs, notamment par le fait qu'elles peuvent développer des interfaces extrêmement conviviales, rassurantes et personnalisées en fonction du profil de chaque utilisateur qui, de fait, peut ainsi se sentir, au fur et à mesure, de plus en plus chez lui lorsqu'il interagit avec des plateformes qui le reconnaissent, un peu à la manière dont on peut se sentir chez soi lorsque, dans un bar ou dans un restaurant où l'on aurait ses habitudes, le serveur nous apporte, sans que nous ayons rien eu à commander, notre boisson favorite.

Je me demandais, de ce fait, s'il ne serait pas temps de réfléchir sérieusement au rôle et à la responsabilité des *designers* dans la conception de ces interfaces, en raison de leur capacité à générer de la confiance dans l'économie numérique, confiance fabriquée sans être enracinée dans aucune routine des relations, ni justifiée par aucune assurance ni consciemment décidée.

J'avais une autre interrogation. Parmi les obligations relevant du principe de loyauté, il existe l'obligation de notifier aux acteurs professionnels les changements réalisés dans les algorithmes de traitement des données (classifications, référencements, etc.) et je ne comprends pas très bien pourquoi cette obligation n'est pas étendue aussi vis-à-vis des utilisateurs des réseaux sociaux ? Par exemple, « *Timeline* » (en français « Journal ») a changé en profondeur l'interface utilisateur de *Facebook*, ce qui a affecté l'ensemble des utilisateurs. Ceux-ci peuvent perdre quelque peu la

127 B. Six, *Des théories libérales du choix rationnel à la gouvernance du fait social monétaire*, P.I.E. Peter Lang, 2013, coll. « Philosophie et Politique », N.25, p. 106-107.

128 Pour une description fine des différents types de confiance et de leurs implications sociétales, v. notamment B. Six, *Des théories libérales du choix rationnel à la gouvernance du fait social monétaire*, P.I.E. Peter Lang, 2013, coll. « Philosophie et Politique », N.25, ainsi que C. Lobet-Maris, R. Lucas et B. Six (dir.), *Variations sur la confiance*, P.I.E. Peter Lang, coll. « Philosophie et Politique », N. 18, 2009.

maîtrise des trajectoires des informations qu'ils exposent, dans la mesure où ils ne savent pas, n'ayant (par hypothèse) qu'un seul compte, comment ils vont être vus ou perçus par autrui.

Lorsque l'on génère volontairement du contenu sur Internet, on a souvent un type de destinataires en tête. Il arrive que l'on exclue volontairement certaines personnes – sur *Facebook*, par exemple, il est possible de rendre certains contenus invisibles pour certaines personnes –. Mais, alors que l'on aurait voulu n'exclure personne, et publier certaines choses à destination de la totalité de nos contacts, il se peut fort bien que la plupart d'entre eux ne voient jamais ce que nous avons publié, dans la mesure où l'algorithme aura fait à leur place, ainsi qu'à la place de l'émetteur, le choix d'exclure le contenu en question du fil d'actualité algorithmiquement évalué comme pertinent pour tel ou tel lecteur. En tant qu'émettrice du contenu, je suis incidemment trompée sur l'acoustique du réseau social. Je crois parler très fort pour tout le monde alors que je chuchote à l'oreille de quelques uns. Dans ce contexte, il est donc nécessaire et utile que les utilisateurs des réseaux sociaux soient avertis des transformations qui peuvent survenir dans les règles qui définissent l'acoustique de ces endroits particuliers.

Nicolas Colin
Inspecteur des finances, entrepreneur

La question de la confiance est à la fois une question centrale dans la compréhension de l'économie numérique et l'une des plus mal traitées. Je fais partie des gens qui regrettent systématiquement le raccourci abusif pratiqué entre les notions de confiance et de sécurité. Et si l'on collecte des informations et qu'on les analyse, on s'aperçoit que la surenchère dans la sécurité n'est pas du tout de nature à renforcer la confiance ; elle peut même avoir l'effet inverse, l'utilisateur se posant beaucoup de questions sur les risques encourus, réels ou supposés.

Sur la formulation de votre question, je m'interrogeais sur la notion de « *nouveaux entrants* » qui désignent de nouvelles entreprises arrivant sans cesse sur le marché. Toutefois, les entreprises qui opèrent sur les grandes plateformes de l'économie numérique ne sont pas si nouvelles que cela : *Amazon* a été créé en 1994, il y a vingt ans, *Google* en 1998, *Facebook* en 2004 et *Apple* en 1976. Je ne suis donc pas sûr, dans la cas particulier de ces entreprises, que l'on ne soit pas en présence d'une confiance routinière de la part des utilisateurs, d'autant plus qu'aujourd'hui les internautes restent connectés en permanence par leurs téléphones mobiles; une confiance routinière peut donc s'installer en quelques jours. On peut en effet utiliser quelques jours une nouvelle application, s'apercevoir le produit répond à nos besoins, que notre boîte courriel n'est pas envahie de courriers indésirables, que le service rendu est conforme à la proposition de valeur et que le prix correspond à ce qui était prévu. Comme toujours dans le numérique, il n'y a pas grand-chose de nouveau mais on change d'échelle, c'est l'intensité de l'interaction qui fait qu'une confiance routinière s'installe beaucoup plus vite.

Cela étant dit, il y a aussi un immense savoir-faire dans l'économie numérique sur la conception (en anglais, « *design* ») de l'interface utilisateur, conçue pour séduire, qui puise son inspiration dans deux sources :

La première source est le savoir-faire des concepteurs et le raffinement de leur savoir-faire, qu'ils mettent directement en prise avec les utilisateurs observés en temps réel. C'est la différence radicale entre les produits développés dans l'ancienne économie numérique (le monde informatique primitif) qui étaient gravés sur cédéroms et vendus *via* des magasins : quand les utilisateurs installaient ces logiciels et les utilisaient, il était impossible de savoir ce qui se passait. À l'inverse, quand un utilisateur utilise aujourd'hui une application par l'intermédiaire d'un navigateur ou d'un téléphone mobile, on observe en temps réel ce qui se passe, et l'on détecte immédiatement la dégradation de la confiance si, par exemple, un menu n'apparaît pas au bon endroit ou si une information demandée revêt un caractère trop intrusif. Non seulement le concepteur propose, dès le début, une interface utilisateur aussi sophistiquée que simple d'usage, mais encore, il peut la modifier en temps réel ou dans des délais très courts, pour en corriger les biais, en gommer les imperfections, optimiser une expérience et proposer rapidement une mise à jour, ce qui me semble relever de la confiance routinière.

La deuxième source est une idée plus atypique, que je continue de défendre : l'économie numérique est dominée par des entreprises américaines qui appartiennent à un pays où la culture du service a un sens sur les marchés de masse, alors que nous sommes, en France, un pays où la culture du service n'existe que sur une niche, celle des clients de l'industrie du luxe. C'est très français : on aime beaucoup ces systèmes privilégiés où une petite minorité est bien servie, et où les autres doivent se contenter des restes, que ça leur plaise où non. Cela est présent à tous les niveaux de la société comme en témoigne, par exemple, la dichotomie entre les grandes écoles et les universités. Cela se voit aussi avec les différences de traitement sur les marchés de masse où l'on est mal traité, où il existe des files d'attente insupportables (les médecins spécialistes...), où l'on est dans l'incapacité de négocier quoi que se soit, insulté et maltraité par des serveurs de café ou des chauffeurs de taxi, etc.

À l'inverse, certains d'entre nous ont pu faire l'expérience, aux États-Unis, de cet environnement beaucoup plus feutré et agréable où tout le monde est attentif et aux petits soins avec le client. Je trouve d'ailleurs les français qui voyagent aux États-Unis assez désarmés par cette prévenance qui marque les services rendus au quotidien ; à tel point qu'elle suscite même une sorte de méfiance envers autrui et une interrogation quant à la contrepartie à offrir à cette insistance à vouloir si bien servir le client. Or, la société américaine est conçue comme cela pour des raisons culturelles et économiques. Le fait que l'économie numérique soit dominée par les américains a installé cette culture de la prise en compte personnalisée des besoins des clients pour tenter d'y répondre au mieux. Il s'agit là du principal moteur de la confiance dans une entreprise qui, manifestement, fait de gros efforts pour comprendre qui est le client et essayer d'adapter son offre à ses besoins.

Un autre élément inspire confiance dans l'économie numérique : la réactivité. Ce que les concepteurs appellent « *responsiveness* », c'est-à-dire le fait que, quand le

client proteste, l'entreprise réagit en lui répondant immédiatement. Ce n'est pas du tout comme en France où l'on se trouve face à une bureaucratie qui, du haut de ses compétences supposées, vous considère comme un intrus ; où l'on a beau écrire des lettres, interpeller le guichetier, etc., il ne se passe rien. Le sentiment qui domine n'est pas la confiance mais l'impuissance.

Certes, dans l'économie numérique, si l'on est seul à protester face à un milliard d'utilisateurs satisfaits, il ne se passera rien. Mais si quelques dizaines de milliers de personnes protestent en même temps, les entreprises du numérique, comme par exemple *Facebook*, le mesurent et corrigent instantanément ce qui ne va pas. Cette réactivité est extrêmement rassurante, car elle apaise les utilisateurs qui se savent « *écoutés* » (*sic*) et satisfaits de ne pas être obligés de protester plusieurs fois pour la même demande. Il me semble que, sur les ressorts de la confiance, tous ceux qui confondent confiance *et* sécurité sont les mêmes que ceux qui pensent que les français ont plus confiance dans leur banque qu'ils n'ont confiance dans *Google*. Mais la réalité est ainsi faite que les banques, les opérateurs de télécommunications ou un certain nombre d'entreprises traditionnelles sont les entreprises les plus haïes par leurs clients ! Et le fait que les clients restent n'est pas dû à la confiance qu'elles inspirent, mais à un ensemble de rigidités de marché que l'on connaît bien en France et qui font qu'il est (quasiment) impossible de quitter la sécurité sociale, sa banque, de résilier son engagement envers son opérateur télécoms, etc.

À titre personnel, j'ai été marqué par une personne qui, chez *Google*, dirigea un service appelé : *le front de libération des données*. Cette personne m'a certifié que son entreprise ne vend pas les données de ses utilisateurs à d'autres sociétés, contrairement à ce qui se pratique couramment aux États-Unis. En effet, lorsque vous êtes, par exemple, client d'une banque, la banque vend son fichier de clients à de nombreux partenaires qui, ensuite, vous envoient des courriers, regardent si vous êtes riches ou pauvres, si vous avez un prêt hypothécaire, un découvert, etc.

À travers ces exemples, nous réalisons que les pratiques ouvertement affichées des entreprises de l'économie numérique sont un progrès considérables par rapport à celles des entreprises traditionnelles.

Laurent Cytermann
Maître des requêtes au Conseil d'État

Je suis d'accord avec vous.

Francis Donnat
Directeur des relations institutionnelles
et des politiques publiques de Google France

Je souhaiterais faire trois observations pour nourrir le débat. Tout d'abord sur la concurrence du secteur, je ne peux aller que dans le sens de ce qu'a dit Nicolas Colin. À cet égard, on se plaît à citer un article de la revue *Fortune* qui titrait en 1998 « *La guerre des moteurs de recherche est finie, et c'est* Yahoo *qui l'a remportée* », au moment même ou Sergueï Brin et Larry Page étaient en train de mettre au point leur programme *PageRank*, alors qu'ils étaient étudiants à l'université de Stanford, et de fonder ensuite *Google*.

Toujours pour aller dans le sens de Nicolas Colin, il faut distinguer les différents services et les différentes plateformes. Dans le cadre du moteur de recherche, on constate que personne n'est obligé d'utiliser tel ou tel moteur de recherche, que les coûts de transaction ou la difficulté du passage d'un moteur de recherche à un autre sont nuls, contrairement à d'autres activités, de sorte que nous disons souvent que « *la concurrence est à un clic* ». Il n'y a pas non plus à proprement parler d'effets de réseau: je n'utilise pas *Google* parce que mes amis l'utilisent, mais parce que je trouve le résultat de ses recherches pertinent.

Il n'y a donc pas ici d'effets réseaux ou de barrière à l'entrée notamment en terme de données, ni d'ailleurs en terme financier ou culturel. Lorsque *Google* a commencé, c'était précisément *Yahoo* l'entreprise la plus importante. Cela n'a pas empêché *Google* de décoller très rapidement car le produit était innovant et, surtout, les algorithmes ainsi que les services étaient meilleurs. Comme dit le proverbe : « *la recette est plus importante que les ingrédients* ». On le voit encore aujourd'hui lorsque de nouveaux entrants arrivent sur le marché pour proposer leurs services: ils n'ont pas à leur disposition des masses de données énormes, mais simplement une idée innovante qui leur permet de gagner progressivement des parts de marché.

Ensuite, c'est un secteur dans lequel la concurrence est vive. À supposer qu'on accepte de considérer qu'il y a aujourd'hui un marché de la recherche en ligne, celle-ci est aujourd'hui multifacette et ne consiste plus seulement en une recherche sur la barre de saisie d'un ordinateur. Cette recherche est d'abord commerciale, *via eBay* ou *Amazon* – d'ailleurs on peut noter que 30 % des recherches commerciales commencent et s'achèvent sur *Amazon*. La recherche, c'est aussi les réseaux sociaux : *Twitter*, *Facebook* et d'autres – un adulte sur trois accède à l'information via *Facebook* et *Pinterest* représente actuellement 25 % de l'activité de partage social sur Internet. Tout cela caractérise la recherche qui concerne aussi des acteurs qui sont plus jeunes encore que ceux qui ont été cités par Nicolas Colin.

Ma deuxième observation porte sur la notion d'infrastructure essentielle. La Cour de justice de l'Union européenne (CJUE) – anciennement Cour de justice des Communautés européennes (CJCE) – avait fixé à l'époque des critères pour définir ce qu'est une infrastructure essentielle dans des arrêts de 1988 et 1995[129]. On ne retrouve pas ces éléments lorsque l'on parle des plateformes numériques. L'accès aux installations doit être un élément indispensable. Or, dans le monde numérique il n'existe pas de point d'entrée unique vers Internet, mais de multiples points d'entrée. Il n'y a pas non plus de barrières insurmontables à l'entrée, ni en termes financiers, ni en termes de données. La reproduction des infrastructures ne se fait pas à un coût prohibitif, comme le prouvent les entrées régulières de nouveaux prestataires et la création de nouveaux services.

Enfin, ma troisième observation fait échos à ce qu'a dit Laurent Cytermann concernant l'Allemagne et le groupe de presse *Axel Springer*. Les chiffres montrent, par exemple, que le journal *Bild* tire 70 % de son trafic quotidien depuis l'accès direct à son propre site Internet, puis environ 10 % *via* les moteurs de recherches

129 CJCE, aff. C-238/87, 5 octobre 1988, *Volco c. Veng* ; CJCE, aff. C-241/91 et C-242/91, 6 avril 1995, *Magill*. V. aussi CJCE, aff. C-418/01, 29 avril 2004, *IMS Health*.

et le reste à travers les réseaux sociaux *Twitter* ou *Facebook*. Ce qui démontre qu'il n'y pas véritablement de point d'entrée unique ou de gardien de l'Internet, comme on l'a également constaté en Espagne après la fermeture (récente) de *Google actualité* qui n'a pas fait chuter le trafic vers les sites de la grande presse ; alors qu'en revanche les petits éditeurs qui tirent davantage leur trafic des moteurs de recherches en ont pâti.

Nicolas Colin
Inspecteur des finances, entrepreneur

Contrairement à Francis Donnat, je ne suis pas d'accord sur l'absence d'effets de réseau sur les moteurs de recherche. J'aimerais vous donner un seul exemple que je tiens de Fréderic Kaplan qui avait fait une présentation remarquable, il y a deux ans, lors d'un évènement organisé par l'Institut de recherche et d'innovation du Centre Pompidou : l'autocomplète des requêtes de recherche[130].

Aujourd'hui, il n'a échappé à personne que lorsque vous commencez à saisir votre requête ou une chaîne de caractères, par exemple dans *Google*, l'application vous propose une manière de compléter vos mots clés. Cette autocomplète est un effet de réseaux parce que beaucoup de personnes ont soumis, avant vous, une requête qui, commençant par votre mot, s'est terminé d'une certaine façon, et que ces personnes ont été satisfaites de la réponse placée en tête par *Google*. Cela paraît n'être qu'une mini-fonctionnalité qui fait gagner quelques dixièmes de secondes dans la soumission de la requête. Mais, en réalité, cela génère un effet de réseau au sein du moteur de recherche : parce qu'il y a beaucoup d'utilisateurs, le moteur de recherche vous propose une autocomplète pertinente ; à l'inverse, s'il y a peu d'utilisateurs, le moteur de recherche ne propose pas cette autocomplète. C'est pourquoi, au final, l'utilisateur adoptera l'outil qui lui facilite la tâche et lui permet de saisir sa requête plus rapidement.

Christian Paul
Député de la Nièvre, coprésident de la commission de réflexion sur le droit et les libertés à l'âge du numérique

Je vous propose de continuer les interventions et d'élargir la réflexion à d'autres plateformes que les moteurs de recherche.

Francis Donnat
Directeur des relations institutionnelles et des politiques publiques de Google France

Sur la notion de plateforme, vous m'avez demandé d'apporter le point de vue de l'entreprise que je représente, et je voudrais insister sur deux aspects. Le premier élément est la très grande diversité des services qui, susceptibles d'être qualifiés

130 *L'autocomplète* ou *le complètement automatique* est une fonctionnalité informatique permettant à l'utilisateur de limiter la quantité d'informations qu'il saisit avec son clavier, en se voyant proposer un complément qui pourrait convenir à sa chaîne de caractères..

de plateforme, créent une interrogation : est-ce qu'une notion aussi englobante est véritablement utile face à une telle diversité de services qui relèvent chacun d'un régime juridique existant et déjà appliqué ?

Le second élément porte sur la notion de loyauté qui, selon moi, intègre les aspects de *portabilité* et d'*interchangeabilité* entre les systèmes, constitutifs de la loyauté entre les acteurs économiques. D'abord, *Google* comme beaucoup d'autres entreprises proposent de très nombreux services qui, par leur diversité, relèvent de régimes juridiques distincts, ce dont ne rend pas compte la notion de plateforme qui semble vouloir coller une étiquette unique sur des éléments différents. En voici quelques exemples. Au sein du moteur de recherche, il y a les résultats naturels qui sont les résultats algorithmiques et, affichée sur le côté de façon signalée et transparente, il y a la publicité contextualisée que *Google* offre. Rien que cela fait déjà coexister deux régimes juridiques distincts car avec la publicité nous sommes dans un régime de contrats publicitaires avec nos partenaires. À l'autre extrémité de notre palette de services, il existe un service de musique appelé *Google Play Music* qui permet l'accès à des contenus musicaux au travers d'abonnements (un peu comme *Deezer*). C'est un régime juridique totalement différent d'accès à des contenus musicaux. Au milieu de ce spectre, il y a *Youtube*, que Laurent Cytermann a cité précédemment. Tout le monde connaît cette plateforme de partage de contenus mais, en réalité, il y a beaucoup de services offerts sur *Youtube* et qui relèvent chacun d'un régime juridique différent.

Nicolas Colin disait que parfois les utilisateurs inventent avec nos services des usages auxquels nous n'avions pas pensé. Le premier d'entre eux, utilisé avec *Youtube*, est de réaliser du stockage de vidéos pour soi-même. Pour cela, il suffit de mettre en ligne une vidéo et de ne la partager avec personne. Dans ce cas le régime est celui du contrat du louage d'espaces et de services. Ensuite, il y a le service *Youtube* qui permet d'échanger des vidéos avec des personnes : au lieu d'envoyer une vidéo en pièce jointe avec votre courriel, vous mettez en ligne une vidéo et vous ne la partagez qu'avec une ou plusieurs personnes. C'est un autre usage de *Youtube* qui s'apparente au régime de la correspondance. Troisièmement, on a le service classique de *Youtube* qui permet à des amateurs de mettre en ligne des vidéos. Actuellement, trois cents heures de vidéos nouvelles sont mises en ligne chaque minute avec descriptions et commentaires. On relève là du régime de l'hébergement. Quatrièmement, toujours sur *Youtube*, il existe un service qui n'a pas encore été lancé en France, *Music Key*, qui est une espèce de *Youtube* payant, sans publicité, avec écoute en ligne (en anglais « *streaming* ») ou possibilité de télécharger musique et vidéos pour en profiter hors connexion. C'est un peu l'équivalent de *Deezer*. Cette application relève d'un régime de services différent. Enfin, *Youtube* permet de diffuser des contenus en direct et là nous ne sommes pas hébergeurs, car il n'y a pas de stockage, mais intermédiaires techniques car c'est le diffuseur qui utilise notre technologie dite de *streaming* qui est le responsable éditorial du contenu diffusé en direct *via Youtube*.

Au regard de cela, je souhaiterais introduire deux notions que l'on a peu abordées et qui me semblent importantes pour la loyauté dans les relations économiques entre les acteurs : l'interopérabilité des systèmes et la portabilité des données.

L'interopérabilité des systèmes est une notion qui est utilisée pour décrire un modèle ouvert qui permet à différents produits et services de fonctionner correctement sur une même plateforme. C'est le choix fait par *Google* en développant le système *Android* qui est un modèle ouvert, une plateforme qui permet aux créateurs d'applications de développer des services qui fonctionnent de manière homogène. Si, par exemple, vous voulez changer de messagerie sur votre plateforme *Android*, il y a un système extrêmement facile pour passer d'une application de messagerie à une autre, l'utilisateur pouvant contrôler tout ce qu'il installe. Les développeurs savent qu'ils ont un modèle de plateforme totalement ouvert où ils peuvent, de façon parfaitement libre, développer et mettre en ligne des produits nouveaux.

La portabilité est un autre élément dans lequel nous croyons énormément : *Google* travaille de façon à permettre à ses utilisateurs et à ses partenaires commerciaux d'adopter les produits et les services des concurrents aussi facilement qu'ils ont adopté les nôtres. Pour l'utilisateur, c'est ce que nous appelons le front de libération des données *Google* (en anglais, « *Google data liberation front* ») qui s'est traduit par un produit que l'on appelle le « *Google takeout* » et qui permet en quelques clics aux utilisateurs de *Google* d'exporter leurs courriels, leurs contacts, leurs photos et leurs contenus numériques (magazines, livres, vidéos) dans des formats standards pour migrer vers des services concurrents. Nous avons mis exactement la même chose en place avec les services de campagne publicitaire, qui peuvent être exportés *via* des formats standards vers des services concurrents.

Portabilité des données et interopérabilité des systèmes constituent donc des éléments de nature à garantir la loyauté dans les rapports économiques entre les acteurs, parce qu'ils offrent aux utilisateurs le choix de leurs outils numériques, aux nouveaux acteurs le libre accès aux plateformes ou des opportunités nouvelles, et aux acteurs établis une ardente incitation à ne pas cesser d'innover.

Antoinette Rouvroy
Chercheuse qualifiée au centre de recherche en information, droit et société de la faculté de droit de Namur

Afin d'envisager, dans leurs ramifications complexes, les enjeux d'un principe de loyauté des « *plateformes* » (loyauté envers qui ? Obligeant à quoi ? Sanctionnée comment ?), je voudrais principalement évoquer *les propriétés algorithmiques de l'espace public numérique* (un espace intensément participatif, mais aussi intensément privatisé, etc.) et les transformations de cet espace public, en raison de l'avènement des plateformes au rang d'acteurs dominants du partage de données (y compris des données sensibles) et, à ce titre, jouant le rôle de gardien ou de guichetier (en anglais, « *gatekeeper* »), à la fois pour les utilisateurs (dont ils façonnent l'expérience, c'est-à-dire l'accès à l'information, la forme des interactions sur les réseaux sociaux, etc.) et, potentiellement, pour toute une série de clients (annonceurs commerciaux, compagnies d'assurance, entreprises, gouvernements, etc.), acquérant gratuitement ou contre paiement un droit d'accès plus ou moins étendu et/ou un droit d'utilisation des données (anonymisées ou non) détenues par les plateformes[131].

131 *Google*, par exemple, est financé en grande partie par la publicité et offre aux publicitaires

Dans un deuxième temps, j'essaierai de dire quelques mots du *r*égime spécifique des plateformes et donc du principe de loyauté et des obligations qui en découlent : obligation de pertinence pour fournir le meilleur service à l'utilisateur et obligation d'information sur les critères de classification et de référencement, avec leurs ambivalences et leurs difficultés d'application au regard des spécificités algorithmiques des espaces publics numériques. J'aurais aimé évoquer aussi, si j'avais eu plus de temps, la piste suggérée dans l'étude du conseil d'État, d'un « *droit des algorithmes prédictifs* ». En effet, bien qu'ils ne s'y réduisent pas, les algorithmes sont au cœur du fonctionnement des plateformes. Je tenterai d'en dire quelques mots en filigrane dans mon exposé.

Les propriétés de l'espace public algorithmique

Tout d'abord, intéressons-nous aux propriétés de l'espace public algorithmique et aux manières dont il diffère d'un espace public politique. On a cité précédemment l'invention de l'algorithme *PageRank* par MM. Sergueï Brin et Larry Page alors qu'ils étaient encore étudiants à Stanford. L'algorithme est fondé sur une présomption assez simple : chaque fois qu'une personne cite ou fait référence à une autre page sur un autre site, il exprime un jugement de pertinence ou d'intérêt, renforçant ainsi la *réputation quantitative* des pages concernées. Chaque lien hypertexte comporterait donc un peu d'intelligence humaine, de sorte que tous les liens combinés formeraient une espèce d'intelligence collective ; ce qui signifie qu'à chaque fois qu'un individu crée un lien ou clique sur un lien, il nourrit *l'intelligence* du moteur de recherche[132].

Tout cela se fonde sur une vision particulière de ce que sont l'information, le savoir, l'intelligence, vision dans laquelle les modes de véridiction et d'évaluation classiques (qu'il s'agisse des modes d'évaluation propres à la critique culturelle, des modes de véridiction propres à la méthode scientifique, ou encore des modes de vérification propres aux pratiques des journalistes) sont remplacés par un classement en fonction de *l'utilité* présumée de chaque contenu pour chaque utilisateur, utilité établie en fonction, d'une part, de la réputation quantitative des contenus, qui permet leur *hiérarchisation* (en fonction de la quantité de clics et de renvois (citations) générés par chaque page ou document) et, d'autre part, du profil singulier de chaque utilisateur, produit par l'analyse automatisée de son historique de navigation, de ses relations et interactions sur les réseaux sociaux, etc., et qui permet la *personnalisation* des contenus. *In fine*, il s'agit de produire une auto-organisation du savoir immanente au monde numérisé à travers l'action de l'ensemble des individus de la société connectée, en même temps qu'une personnalisation des environnements informationnels censée maximiser *l'utilité* de/pour chaque internaute sans en passer par aucun échange langagier avec lui ni par aucune proposition ni énonciation volontaire d'intérêt ou de besoin.

---

des services de ciblage très performants. La nouvelle loi française sur les services de renseignement prévoit différentes modalités d'accès pour les services de renseignement aux données détenues par les plateformes. *Apple* aurait approché, en 2014, plusieurs entreprises d'assurance santé aux États-Unis pour leur vendre les données récoltées sur sa plateforme de santé connectée, ...

132 À propos de l'algorithme *PageRank*, lire D. Cardon, « Dans l'esprit du PageRank. Une enquête sur l'algorithme de Google », *Réseaux*, 2013/1 (N.177), pp. 63-95.

Je voudrais insister sur cette notion d'immanence : l'hyperfragmentation et la croissance exponentielle de l'univers numérique substitue de nouvelles possibilités de modélisations (des comportements, des propensions, des trajectoires, etc.) immanentes et simultanées plutôt qu'extérieures et antécédentes aux traitements de données. L'évaluation de l'utilité et de la fiabilité (plutôt que la vérité ou la validité) des pages ou documents n'est plus tributaire de systèmes qui feraient intervenir des structures, formes, catégories instituées (socialement, politiquement, scientifiquement) antécédentes et extérieures à l'écosystème numérique. La rationalité algorithmique semble s'être émancipée des systèmes de perception et d'interprétation du monde précédemment fondés sur des phénomènes de représentation (symbolisation, institutionnalisation, etc.) et de recognition de structures, formes, catégories (politiquement, juridiquement, culturellement) instituées.

Les « *plateformes* » sont les acteurs privilégiés de la révolution informatique qui, dans ses ambitions contemporaines dominantes (le tournant numérique, les mégadonnées, l'exploration de données, etc.), n'est pas la cause mais le symptôme d'une « *passion pour le réel* » ; non pas pour un réalisme de la représentation, mais pour le réel comme tel, pour un accès immédiat au monde qui ne passerait plus même par le langage, qui ne dépendrait plus d'aucun régime de vérité (Foucault) : le territoire numérique deviendrait sa propre carte, un sismographe au diapason des frissons d'un monde devenu modélisable jusque dans ses recoins d'incertitude irréductible. Pour prendre exemple, l'algorithme *PageRank* – cela vaut aussi pour tous les algorithmes utilisés par *Google*, *Facebook*, etc. – se présente comme totalement neutre sur le plan des jugements de valeur. Il fonctionne sur une logique de *comportementalisme numérique*, à travers des traitements de données purement algorithmiques et/ou quantitatifs (le nombre de liens entrant sur chaque page va déterminer la pertinence et donc le rang de classement) qui peuvent se compléter avec un aspect relationnel, plus social (personnalisation). Cette objectivité machinique, qui pourrait sembler émancipatrice en ce qu'elle offrirait – enfin – une sorte d'accès *immédiat*, sans médiation, direct, objectif, non biaisé au *réel*.

Cette immanence, ce régime de fiabilité sans vérité[133] ou cette « *intelligence collective* » (qui est en fait un régime de *vérité* dans lequel on ne cherche pas la vérité, mais seulement une certaine opérationnalité et qui se révèle plus proche de stratégies d'optimisation que de processus de production de savoir) semble pouvoir dispenser des processus de véridiction propres aux domaines scientifiques tout autant que des processus de légitimation propres aux domaines politiques. L'idée de l'auto-organisation du savoir, à laquelle participent *tous* les utilisateurs « *à égalité* » quelles que soient leurs compétences, promeut la vision d'un *résultat naturel*. On se trouverait donc dans un nouvel état de nature (« *automatic is the new natural* », pourrait-on dire en anglais), alors que la détermination des critères de hiérarchisation et d'évaluation de l'utilité (de tout ce qui se laisse numériser) appartient de fait, en raison de la masse des données qu'ils traitent, à de très grands acteurs de l'Internet qui ne se présentent pas du tout comme des *acteurs de gouvernement*, mais comme de *simples entreprises* dont les catégorisations

133 Sur le *régime de vérité numérique*, v. notamment A. Rouvroy et B. Stiegler, « Le régime de vérité numérique : de la gouvernementalité algorithmique à un nouvel état de droit », *Socio*, 2015, N.4, 113-140.

et hiérarchisations ne feraient que refléter une normativité immanente au social lui-même, ce qui, d'ailleurs, rappelle assez bien la description du pouvoir par Michel Foucault : le pouvoir n'est jamais aussi efficace que là où il se fait le plus oublier… L'algorithme *PageRank* de *Google* est, à ce titre, exemplaire : son aura de fiabilité et d'impartialité dépend de l'absence d'intervention humaine (au niveau de *Google*) dans le classement *naturel* (résultant du *comptage* des clics et des liens entrants). C'est à une nouvelle critériologie que nous avons à faire, dans laquelle les critères de classement et de hiérarchisation ne président pas au traitement des données, mais en résultent mécaniquement, ce qui fait disparaître toute impression d'intervention humaine active volontaire. Dans l'espace public algorithmique, les éléments faisant du jugement humain – qui se fonde sur les catégories ou critères toujours incertains, constamment renégociés, exigeant un débat constant – quelque chose de relativement *critique* sont éliminés.

L'espace public algorithmique est donc un espace paradoxal, qui peut sembler à la fois extrêmement *démocratique* (tout le monde participe quel que soit son statut social, sa formation, son niveau de compétence, son intention), mais dans lequel les critères d'évaluation ne résultent d'aucune délibération publique, mais sont *produits* de manière immanente et automatique, à même les *données* après avoir été *traduits* en termes *d'utilité*.

C'est à l'endroit, notamment, du calcul et de la caractérisation de l'utilité que surgit la question de la loyauté dans toute sa complexité. Cette notion d'utilité est, en effet, ambivalente dans le contexte des *services* offerts par les plateformes. Car le calcul d'utilité de chaque contenu *pour* l'utilisateur (sa propension à cliquer sur tel ou tel type de contenu) – qui passe par un profilage – permet également de classer chaque utilisateur en fonction des opportunités et des risques, de l'intérêt ou de l'absence d'intérêt qu'il représente lui-même, en tant que consommateur (potentiel), employé (potentiel), assuré (potentiel), fraudeur ou criminel (potentiel) etc., pour une série de *clients* de la plateformes, c'est-à-dire les entreprises et les institutions à qui la plateforme *cède*, à titre onéreux ou gratuit, les données recueillies dans le courant de son activité, et qui peuvent être des annonceurs, des assureurs, des employeurs, des gouvernements, etc. Or les intérêts des utilisateurs, d'une part, et ceux des plateformes et de leurs clients, d'autre part, ne sont pas nécessairement alignés.

Ainsi, par exemple, l'analyse algorithmique de tout ce qui transite sur/par les plateformes permet-elle l'émergence de nouvelles stratégies de persuasion (marketing commercial, électoral, etc.) qui, au lieu de reposer sur l'argumentation rationnelle à destination d'individus supposés capables d'entendement et de volonté (sur le modèle libéral de l'individu libre, rationnel, autonome), repose bien d'avantage sur l'exploitation des *biais*, des *irrationalités* des propensions les moins contrôlées des individus, de tous ces *écarts* par rapport au modèle de l'individu rationnel, écarts devenus détectables, modélisables, exploitables à titre d'opportunités commerciales, électorales, gouvernementales au sens large, etc.). Dès lors, la question qui se pose est celle-ci : dès lors qu'elles sont détectables et exploitables, donc *utiles*, dès lors qu'elles constituent des opportunités de profit commercial, de réduction des coûts, d'optimisation des ressources humaines, etc., est-il légitime et conforme au principe de loyauté que les *irrationalités* des

individus – celles-là même qui s'expriment à travers leurs propensions à agir contre leur propre intérêt (sont visées ici par exemple toutes les formes d'addictions) – ou, tout simplement, les *profils de personnalité* établis sur base de leurs activités en ligne, puissent être exploitées à leurs dépends ?

Ces mêmes analyses algorithmiques permettraient également aux assureurs, par exemple, s'ils pouvaient accéder aux jeux de données traitées par les plateformes, d'obtenir, à propos de leurs assurés ou des candidats à l'assurance, des informations beaucoup plus précises que celles auxquelles ils ont actuellement accès à travers les questionnaires remplis par les candidats à l'assurance. C'est alors toute l'architecture informationnelle du secteur de l'assurance qui risque de basculer, mettant à mal l'équilibre informationnel entre assureur et assuré (lequel équilibre, en de nombreux cas, réclame une certaine asymétrie d'information au profit du candidat assuré), garant d'un accès équitable à l'assurance. Ce sont probablement les assurances santé et les assurances vie qui seraient majoritairement touchées. Dans notre société hyper-connectée, d'après les calculs d'*IBM*, au cours d'une vie, un individu devrait produire plus d'un million de gigabits de données sur sa santé. Ces données de santé ne sont plus seulement produites par le médecin, l'hôpital ou l'assurance-maladie, mais aussi par les individus eux-mêmes, qu'ils soient malades ou bien portants, au fur et à mesure que se répandent les gadgets connectés destinés à surveiller en permanence une série de marqueurs physiologiques (rythme cardiaque, poids, calories brûlées quotidiennement, etc.). Les données relatives à l'alimentation, les données de fréquentation des clubs sportifs, les données de connexion à certains sites d'information ou de discussion à propos de la santé, etc., toutes ces données entrent potentiellement dans la catégorie des données relatives à la santé actuelle ou future. Au fur et à mesure que s'accumulent, grâce aux mégadonnées, des corrélations[134] nouvelles entre des éléments *a priori* sans liens avec la santé et le développement de certaines maladies ou la survenance de certains handicaps (modes de vie, habitudes alimentaires, éléments climatiques et environnementaux, etc.), le champ des données qui deviennent sensibles du fait de leur utilisation s'étend à des types de données que l'on n'aurait jamais pensé rattacher à la catégorie des données sensibles. Si une attention particulière doit être accordée aux données relatives à la santé, c'est qu'elles sont, parmi les mégadonnées, au nombre de celles qui croissent le plus vite à la faveur, notamment, des nouveaux marchés, florissants, de la « *santé connectée* ».

Dans ces domaines – *marketing*, assurance, etc. – l'utilité *pour* l'utilisateur est également ce qui peut permettre de transformer l'utilisateur *sujet de droit*, acteur dans l'espace public numérique, en utilisateur *objet de spéculation*, dans un espace numérique théoriquement public mais, en fait, de plus en plus privatisé. À terme, les critères de mérite, de besoin, de désirabilité, d'acceptabilité ou d'inacceptabilité, bref, les critères présidant à l'accès ou au déni d'accès à certains biens, services, lieux, opportunités, au lieu de faire l'objet d'un débat public, ou d'une délibération collective, seront-ils automatiquement *produits* par les algorithmes ?

134 « *La corrélation, c'est ce qui quantifie la relation statistique entre deux valeurs (la corrélation est dite forte si une valeur a de fortes chances de changer quand l'autre valeur est modifiée, elle est dite faible dans le cas où une valeur a de faibles chances de changer quand l'autre valeur est modifiée* » (J.-P. Karsenty, « Big Data (mégadonnées). Une introduction », *Revue du Mauss permanente*, 1er avril 2015).

Disons-le : le problème du profilage (impliqué notamment dans la personnalisation) n'est pas tant un problème de protection des données personnelles[135], qu'un problème de préservation de l'espace public comme espace de délibération à propos de la chose publique non rabattue sur la seule concurrence des intérêts ou *utilités* privés. Le profilage et la personnalisation parachèvent une sorte d'hypertrophie des espaces et des utilités privés au détriment de l'espace public. Qu'est ce qu'un espace public, si ce n'est un espace dans lequel chacun se trouve confronté à des choses qui n'ont pas été prévues pour lui (en fonction de *son* utilité) ? Le profilage et la personnalisation induisent un *essoufflement* de l'espace public. Bientôt, selon Éric Schmidt[136], il deviendra très difficile pour quiconque de vouloir quelque chose qui n'aura pas été prévu pour lui, tellement les mécanismes de profilage anticipatif vont devenir efficaces. Il est d'ailleurs frappant de constater qu'à l'égard de ce qu'il est convenu d'appeler la « *révolution numérique* », sans doute en raison de l'accession d'un *impératif d'innovation* au statut de logique absolue, les individus se trouvent, le plus souvent, qualifiés de « *consommateurs* » ou d'« *utilisateurs* » dont on promet d'améliorer l'expérience, et beaucoup plus rarement, voir jamais, interpellés en tant que « *citoyens* ». Actuellement, nous sommes donc dans une situation relativement difficile dans laquelle l'espace public est en train de disparaître et où nous perdons une forme de distance nécessaire face à une forme de normativité tout à fait immanente.

C'est que, dès lors que l'on évoque la modélisation algorithmique des comportements humains (par exemple à des fins de marketing, de prévention du terrorisme, de prévention des fraudes, d'ajustement différentiel des prix en fonction de l'élasticité/prix spécifique à chaque consommateur, etc.), modélisation pour laquelle, une fois de plus, les plateformes jouent le rôle de *guichetiers* puisqu'il faut en passer par elles pour obtenir les masses de données suffisantes pour opérer ces types de classifications anticipatrices, ce qui est en jeu c'est la prise en compte ou le mépris de la capacité qu'ont les individus à ne pas se trouver là où ils sont attendus, ou de leur capacité à ne pas faire tout ce dont ils sont capables (et dont témoigne leur *profil*), bref, la dimension de potentialité sans laquelle nous ne ferions jamais l'expérience d'être libres, et sans laquelle nous ne serions jamais différents des « *modèles de comportement* » qui pourraient nous être attribués. La multiplication des profils, leur perfectionnement en *temps réel*, réduit progressivement la distance entre les individus et la somme de leurs profils, au point de faire craindre à terme un état d'indistinction. Cette perte de distance entre l'individu et les *normes* de plus en plus individualisées évoque la

135 Le profilage algorithmique n'implique d'ailleurs pas toujours des données à caractère personnel. Les capacités de mise en relation de données disparates au sein de quantités massives permettent, par détection de corrélations entre données anonymes, de dresser des profils extrêmement précis de comportements auxquels des individus anonymes peuvent correspondre et se voir traiter différemment des autres pour cette raison, sans pour autant être identifiés. Par ailleurs, la notion même de donnée anonyme perd son sens dans le contexte des mégadonnées dans la mesure où, à nouveau, les possibilités de croisement des données permettent, au départ de données anonymes éparses, de réidentifier, avec une marge d'incertitude réduite, la plupart des individus.

136 É. Schmidt, ingénieur en informatique, homme d'affaires, a été président-directeur général de *Google* de 2001 à 2011.

considération, par Cornelius Castoriadis[137], suivant laquelle une norme qui colle à un individu comme une seconde peau est la plus épouvantable des normes parce qu'il devient impossible de prendre de la distance pour la critiquer.

Pour Gérald Dworkin[138], un philosophe du droit américain, la notion d'autonomie implique la possibilité pour les individus, non seulement, d'avoir un libre choix, mais aussi, d'adhérer, de se reconnaître dans les motifs qui les font choisir telle ou telle action. Cela ne veut pas dire que l'on doit, pour être jugé autonome, maîtriser sa propre motivation. Nous savons que nous sommes chacun motivés par divers facteurs sur lesquels nous n'avons pas prise. Mais la possibilité de vouloir être néanmoins motivé par ces facteurs sur lesquels nous n'avons pas prise, est un critère de l'autonomie. Un exemple de choix non autonome est celui du fumeur qui souhaiterait arrêter de fumer, mais se voit proposer systématiquement des publicités pour la cigarette qui risquent de le pousser à en acheter davantage. Sa réelle autonomie – irréductible à l'*utilité immédiate* que revêt pour lui la consommation d'une cigarette, utilité immédiate qui est bien celle qu'identifient les algorithmes dans une économie de l'addiction – sera, même s'il n'a pas prise sur cette avalanche publicitaire qui le cible, en raison, précisément, de son profil de fumeur, parfois aux heures de moindre résistance psychique, de pouvoir résister à sa propre motivation de fumer. Ainsi, assurer la *pertinence* des messages publicitaires est-elle peut-être non pas le *meilleur*, mais le *pire service que l'on puisse rendre à l'utilisateur*. On notera aussi que les *profils* sont extrêmement plastiques ; de sorte qu'à chaque fois que l'internaute s'écarte de la prédiction algorithmique, cela n'est pas considéré comme une erreur ou un échec, mais une occasion supplémentaire de… nourrir la base statistique de manière à améliorer encore la catégorisation des individus.

Le principe de loyauté des plateformes

Il n'est pas certain qu'une obligation de loyauté conçue notamment comme *l'obligation de pertinence destinée à fournir le meilleur service possible aux utilisateurs*, si elle vise fort opportunément à éviter la tromperie volontaire de l'utilisateur au profit, par exemple, d'un *client* de la plateforme, soit pour autant de nature à rendre d'avantage visibles et discutables les enjeux d'autonomie individuelle ni les enjeux collectifs intéressant non le consommateur mais le citoyen, ni à assurer le maintien d'une contestabilité des catégorisations, hiérarchisations et profilages algorithmiques. Alors que la *pertinence* reçoit dans les faits l'acception très réductrice d'une *utilité* calculée d'une manière purement quantitative (comme nous l'avons vu plus haut), l'injonction de pertinence pourrait être perçue comme un encouragement, voir un devoir de profiler le plus finement possible les internautes, et de personnaliser au maximum leurs environnements informationnels, au risque de rendre imperceptibles et indiscutables les enjeux collectifs irréductibles à la seule utilité individuelle (notamment les enjeux de

137 C. Castoriadis (1922-1997) est un philosophe, économiste et psychanalyste. Il consacra une grande part de sa réflexion à la notion d'autonomie.

138 G. Dworkin (né en 1937) est professeur de sciences morales et politiques et de philosophie du droit à l'université de Californie. Il est l'auteur de nombreux ouvrages dont *The Theory and Practice of Autonomy*, Cambridge University Press, 1988.

justice distributive et d'égalité d'opportunités, qui ne manquent pas de surgir dès lors que les profilages sont réalisés au profit de *clients* avides de fonder des distinctions de traitement entre individus sur l'intelligence des données). Ainsi pourrait-on dire que l'opportunité, dans cette logique, tient lieu de valeur finale.

Par ailleurs, l'obligation d'information relative aux critères de classification-référencement mise à charge des plateformes au titre du principe de loyauté paraît difficilement applicable puisque ces critères, précisément, ne précèdent pas les traitements de données mais en résultent. À moins qu'il ne s'agisse d'une obligation de révéler la logique suivant laquelle fonctionnent les algorithmes de classification-référencement, mais alors une telle révélation risquerait fort, d'une part, d'être empêchée par la protection du secret industriel et, d'autre part, de porter atteinte à la fiabilité des classements-référencements, dans la mesure où chacun pourrait, afin d'améliorer son classement ou son référencement, ajuster sa stratégie, ce qui mettrait fortement à mal l'idée du *résultat naturel* sur lequel se fonde l'aura d'objectivité et d'impartialité des classements-référencements algorithmiques. Pour éviter que les utilisateurs n'adoptent des comportements stratégiques visant, par exemple, à gagner quelques places dans les rangs de classement, il est nécessaire qu'ils ignorent, au moins en partie, la manière dont ils sont classés.

Sans doute serait-il envisageable, plutôt que de communiquer ces informations aux utilisateurs, de les communiquer à une instance de contrôle indépendante, qu'il s'agisse d'une autorité de protection des données ou d'une institution *ad hoc*, composée d'informaticiens, de statisticiens et de juristes, par exemple et qui aurait pour tâche d'évaluer le bon fonctionnement des algorithmes, la proportionnalité des atteintes éventuellement portées au principe du respect de l'autodétermination des personnes, et de vérifier qu'ils ne produisent ni n'aggravent des situations de discriminations directes ou indirectes, ni ne nuisent au principe d'égalité d'opportunité.

La question de la non-discrimination est une question difficile : les catégorisations algorithmiques ne se superposant pas explicitement aux catégories socialement éprouvées (comme les catégories établies sur la base de l'origine ethnique, des convictions religieuses, des opinions politiques, du sexe, de l'état de santé actuel ou futur, etc., que les régimes juridiques antidiscriminatoires européens visent tout spécialement), les causes de discrimination éventuelle deviennent relativement invisibles, de même que les probabilités d'actions collectives de protestation contre des discriminations. Pourtant, en prétendant ne faire que refléter les normativités immanentes à la société (numérisée) les algorithmes peuvent très bien refléter aussi les discriminations existantes dans ladite société, voir les amplifier, sans que celles-ci soient reconnaissables en tant que discriminations directes. Dès lors, l'approche antidiscriminatoire retenue dans les instruments de protection des données à caractère personnel consistant à énumérer une liste de *données sensibles*, qui ne peuvent en principe pas faire l'objet de traitements automatisés n'est peut-être pas la plus adéquate pour prévenir la discrimination dans un contexte où, d'une part, les éléments les plus triviaux de la vie quotidienne deviennent, par exemple, potentiellement des indicateurs de l'état de santé actuel

ou future et d'autres caractéristiques sensibles de l'individu et où, d'autre part, les distinctions de traitement entre les personnes peuvent être réalisées de plus en plus finement, sur la base non plus de leur appartenance à tel ou tel groupe historiquement discriminé, mais sur la base d'éléments singuliers de leur mode de vie. Ne serait-il pas utile de considérer qu'au principe de loyauté il faille ajouter la possibilité d'un contrôle qui viserait essentiellement à éviter que les effets des inégalités d'opportunités, induits par l'existence de phénomènes discriminatoires dans la société, ne soient implicitement répercutés et amplifiés à travers les traitements algorithmiques ?

Cette perte de contestabilité[139] des critères de différentiation entre les individus signifie, tant pour les individus qui font l'objet de profilages que pour ceux qui se fondent sur ces profilages pour prendre des décisions à l'égard des individus, un déclin de la responsabilité, allant d'une dispense à une impossibilité de rendre compte des raisons de ses actes ou décisions. Il conviendrait d'identifier de quelle manière, par exemple, l'inversion de la charge de la preuve dans les cas de suspicion de discrimination indirecte, ou encore l'instauration d'un principe général de justiciabilité des décisions prises sur la base de traitements automatisés pourraient contribuer à restituer aux individus leurs capacités à énoncer par eux-mêmes de ce qui les fait agir ou décider de telle ou telle manière alors qu'ils font l'objet de profilages anticipatifs ou qu'ils sont les destinataires de recommandations automatisées.

La formalisation d'un *principe de loyauté imposé aux plateformes* est certainement un pas dans la bonne voie : celle qui mènerait, d'une part, à reconnaître que bien autre chose se joue dans l'espace public numérique que la seule concurrence des intérêts privés, et, d'autre part, à prendre acte et à tenir compte du rôle essentiel, charnière, des plateformes, aujourd'hui véritables guichetières du tournant numérique.

139 V. A. Rouvroy, « The end(s) of critique : data-behaviourism v. due process », in M. Hildebrandt, E. De Vries (eds.), *Privacy, Due Process and the Computational Turn.* Routledge, 2012. Disponible en ligne : http://works.bepress.com/antoinette_rouvroy/44.

Échanges avec les participants

Question *- Ma question concerne surtout la directive sur le commerce électronique. J'avoue ma surprise à la création d'une nouvelle catégorie juridique appelée « plateformes », et j'ai l'impression que cela ressemble à une méconnaissance de la directive ou à une incompréhension de ses objectifs. Les articles 12 à 15 de la directive (il y a quelques articles qui concernent cette responsabilité limitée des hébergeurs) ont été pris car plusieurs juridictions notamment en France avaient, à l'instigation des sociétés de droits d'auteurs, jugé que des sites qui hébergeaient des contenus illicites en termes de droit d'auteur devaient être jugés responsables de cet hébergement, alors même qu'ils n'avaient pas connaissance de ces informations. La directive a répondu de manière extrêmement simple : la responsabilité implique la connaissance des informations. Si vous êtes éditeur à l'origine du contenu, vous en avez nécessairement connaissance. Si vous êtes hébergeurs, vous pouvez en avoir connaissance. Vous en avez connaissance lorsque vous avez un rôle actif, qui peut être le référencement et/ou le classement. C'est ce qu'a jugé la CJUE. La question est donc de savoir si l'on a connaissance du caractère illicite d'un contenu, ce qui permet d'agir pour le faire disparaître. Au final, le cadre de la directive est toujours adapté et il n'y a pas besoin de construire une autre catégorie juridique. La seule question que l'on peut réellement se poser, et cela rejoint les propos tenus par Mme Rouvroy au début de son intervention, c'est si le fait que ce référencement et ce classement, qui interviennent grâce à des algorithmes, impliquent cette connaissance ? C'est cela le vrai sujet, mais il peut être débattu au sein même du cadre juridique existant, ce qui éviterait d'avoir recours à une nouvelle catégorie dont M. Donnat vient de préciser qu'elle englobe des régimes juridiques différents.*

Question *- Avec ces grandes plateformes qui collectent toujours plus de données, de façon toujours plus performante, on a le sentiment d'être surveillé, fiché, devancé dans nos désirs. Vous disiez tout à l'heure que ces sociétés nous connaissaient mieux que nous nous connaissons nous-mêmes. On a vu aussi que le droit courait après ces opérateurs économiques qui sont très puissants. Finalement, est-ce qu'on ne va pas inexorablement vers une société de type « Big Brother » ? Peut-on réguler cette sorte de collecte géante des données ?*

Question *- Ma question s'adresse plus particulièrement à M. Cytermann : vous semblez être d'accord, comme M. Colin, sur la confiance à accorder aux plateformes, sur le caractère bienveillant des services américains à l'égard de tout le monde, sur le caractère très inégalitaire de la société française (illustré par exemple par le contraste entre grandes écoles et universités), sur la confiance des français à l'égard des plateformes de services numériques notamment américaines, ainsi que sur leur détestation des banques et des opérateurs télécoms. Sur quelles études ou éléments statistiques vous appuyez-vous pour être d'accord avec ces propos ?*

Question *- Ma question porte sur les services proposés par les plateformes. Les plateformes liées à la science traitent des intérêts d'une petite communauté, deux millions de publiant au niveau mondial, très structurée et parcourue d'intérêts gigantesques et contradictoires. Au niveau de ces services apparaît une nouvelle catégorie de contenus générés par les utilisateurs pour lesquels nous préparons au CNRS un livre blanc. Ces contenus ont un double enjeu : ils présentent des informations et détaillent leurs traitements qui sont au cœur du travail scientifique. On a besoin de savoir comment cherchent les chercheurs pour chercher soi-même, et les plateformes le permettent. Dans ce contexte, comment peut-on concilier la liberté de commerce et d'industrie et la propriété publique dans le développement de tels services ?*

Laurent Cytermann

À propos des opérateurs télécoms, je remarque que dans une enquête récente, la société Free fait partie des entreprises préférées des Français, mais peut-être est-ce dû à une image plus moderne et à des offres commerciales plus novatrices que celles des entreprises traditionnelles.

Sur la question de la définition juridique des plateformes, est-il nécessaire de créer une nouvelle catégorie relative à la directive commerce électronique ? C'est une question délicate. Je pense que vous avez tout à fait raison de dire que le cœur de la question est de savoir si le fait d'optimiser une présentation, de proposer un référencement d'après un algorithme automatique, caractérise ou non la connaissance des données traitées. Cela renvoie à tout ce que Mme Rouvroy nous a expliqué. Nous avons le sentiment que la probabilité de répondre « oui » à cette question est suffisamment forte pour qu'il soit préférable de fonder ce régime de responsabilité limitée sur un autre fondement, qui nous parait aujourd'hui plus solide et qui prenne en compte le fait que ce sont des services ou des contenus édités par d'autres. Sur cette question, le débat reste ouvert.

Sur la question de la conciliation entre propriété publique et liberté de commerce et d'industrie, je n'ai pas de réponse. C'est une interrogation qui mérite assurément réflexion.

Nicolas Colin

Facebook est une entreprise qui se préoccupe au plus haut point de la conception de son interface utilisateurs, au point que ses concepteurs s'intéressent très fortement au degré de satisfaction des utilisateurs. Il est fondamental pour eux d'avoir ce retour, même négatif, car les aspérités créent et entretiennent également la relation entre l'entreprise et ses utilisateurs. Cette relation est précisément le nerf de la guerre dans l'économie numérique.

Pour cette raison-là, l'idée d'algorithmes qui nous prépareraient une société où tous nos besoins seraient devancés, cette norme dont parlait Castoriadis qui, telle la tunique de Nessus, nous imprègnerait à tel point que l'on n'aurait plus de recul par rapport à elle, n'existe pas. J'en veux pour preuve que dans une société où l'on devancerait vos moindres besoins, on verrait émerger un

besoin nouveau qui serait celui d'être… surpris ! Cela nous emmène dans des raisonnements récursifs un peu compliqués, mais ils montrent que le sens de l'histoire n'est ni univoque ni unidirectionnel.

Sur la confiance, je n'ai pas d'étude particulière à citer, mais chaque fois que l'on évoque les entreprises les plus détestées par leurs clients, je constate que les articles de presse mettent en évidence, dans tous les pays, les banques et les opérateurs télécoms en haut du palmarès.

Je souhaiterais rajouter un point sur la protection des données personnelles. D'aucuns prétendent qu'il serait nécessaire d'empêcher les entreprises de collecter nos données et que, pour cela, il suffirait de durcir la législation. Mais la protection des données personnelles dans la conception française est pourtant claire : on ne peut pas collecter et traiter vos données personnelles sans votre consentement. Il y a ensuite du raffinement sur les conditions d'expression d'un consentement éclairé. Or, durcir la protection des données obligerait les entreprises, pour une finalité donnée, à demander un peu plus l'autorisation des utilisateurs avant de collecter leurs données.

On notera également que dans le cadre actuel, si l'on dispose de données collectées dans un but précis que l'on souhaite utiliser de nouveau dans un autre but, il faut demander à l'utilisateur sa permission.

Quand on dit que l'on va durcir la protection des données personnelles, on oblige les entreprises à se présenter plus souvent devant leurs clients pour leur demander l'autorisation. En conséquence, cela donne une prime évidente aux entreprises qui inspirent confiance. Entre deux entreprises qui demandent l'autorisation de collecte de données, on ne va donner une réponse positive qu'à l'entreprise qui inspire confiance. La réalité est que, du coup, il faut regarder le palmarès des entreprises qui inspirent confiance. On s'aperçoit alors, de manière assez contre-intuitive, que les entreprises qui collectent le plus de données sont également les entreprises qui inspirent le plus confiance pour des raisons de qualité de service, de fluidité des interfaces, de meilleure communication, etc.

Toute démarche visant à rendre plus protecteur le droit des données personnelles doit prendre en compte que cela oblige les entreprises à investir encore plus dans la confiance qu'elles inspirent à leur utilisateur. Et que la meilleure manière de le faire passe par l'amélioration continue du service (personnalisation des prestations, écoute du client, disponibilité) et non pas par les façons traditionnelles de s'attacher un client qui sont caractéristiques de l'économie pré-numérique (engagements, rigidités des contrats).

Antoinette Rouvroy

Je souhaiterais rebondir sur ce qui vient d'être dit. Je ne pense pas que nous puissions être, un jour, exhaustivement profilés. Je le mentionnais dans le cadre de la première obligation mise à la charge des plateformes : l'obligation de pertinence par rapport à un meilleur service. Cela pourrait laisser croire, justement, que l'idéal régulateur serait précisément une parfaite adéquation

du profil à l'internaute. Il va de soi que, comme l'écrivait Spinoza, « on ne sait jamais de quoi un corps est capable ». Les algorithmes ne le savent pas davantage, mais dispensent néanmoins ceux qui s'y fient de la charge de faire face à cette incertitude radicale, de la représenter. Le confort qu'apportent les algorithmes, c'est qu'ils nous soulagent de la tâche de douter, d'hésiter, de rechercher quelle serait la manière de nous tenir dans une position juste relativement à notre propre ignorance. Les algorithmes proposent des solutions qui ne sont ni vraies, ni nécessaires, mais directement opérationnelles. Ils nous dispensent de l'épreuve, éminemment éthique, de l'indécidable.

Quant à la peur de vivre dans une société de type « Big Brother »[140], la situation actuelle, ou celle vers laquelle nous semblons nous diriger, ne correspond pas du tout à celle du roman d'Orwell.

Le gouvernement par les données (que j'ai appelé par ailleurs gouvernementalité algorithmique) est peut-être le plus parfait opposé d'un pouvoir tyrannique qui aurait aboli la liberté de pensée et d'expression (comme dans 1984) : au contraire, ce nouveau mode de gouvernement ne fonctionne bien que parce que les individus se sentent libres de… penser et, surtout, de s'exprimer et donc de semer des données. Alors que dans 1984, « Big Brother » rassemble d'énormes quantités de données à propos de chaque citoyen dans un but précis, les phénomènes de pouvoir (ainsi que les acteurs) qui se nourrissent des mégadonnées sont aujourd'hui beaucoup moins centralisés, beaucoup plus diffus, leurs buts (pour peu qu'il en reste) ne se dessinent qu'en cours de route, l'autorité n'est plus assumée par aucune figure centrale, etc. Bref, on est très loin d'Orwell.

Plus généralement, le recours systématique aux métaphores littéraires de la science-fiction classique, s'il a l'avantage de parler et de faire peur directement à tous (ces figures font partie de notre inconscient collectif), produit des effet d'aveuglements qui stérilisent un peu la pensée critique, lui permettant de ne faire que réactiver, assez paresseusement, les figures de « Big Brother » ou du Meilleur des mondes[141], tout en se dispensant d'identifier exactement les particularités du type de pouvoir qui s'exerce sur les individus et les collectifs aujourd'hui.

Je pense que si nous voulons vraiment comprendre finement ce qui nous arrive, nous avons fortement intérêt – dans la mesure du possible – à cesser de tenter de faire rentrer ce que nous observons dans les moules préétablis des vieux récits/clichés de science-fiction. La question est plutôt de savoir de quel(s) levier(s) nous disposons pour orienter, d'une manière qui nous satisfasse, cette évolution et pour sauvegarder l'idée que nous nous faisons d'un espace public.

140 V. le roman d'E. A. Blair, *alias* G. Orwell (1903-1950), *Nineteen Eighty-Four (1984)*, ed. Secker & Warburg, Londres, 1949 (traduction française : Gallimard, Paris, 1950).

141 V. le roman d'A. L. Huxley (1894-1963), *Brave New World*, ed. Chatto & Windus, Londres, 1932 (traduction française : *Le meilleur des mondes*, Plon, Paris, 1932).

Conclusion de la table ronde

Christian Paul
Député de la Nièvre, coprésident de la commission de réflexion sur le droit et les libertés à l'âge du numérique

En conclusion de ces échanges, je retiendrais deux interrogations.

La première fait écho à votre préoccupation, Mme Rouvroy : faut-il réécrire la directive européenne sur le commerce électronique ? L'intuition du Conseil d'État, présent dans un certain nombre de lieux où l'on débat collégialement de cette question, est qu'il faut arriver à appréhender cette catégorie nouvelle que sont les « plateformes ». En effet, ces entités ne se résument pas à celles que l'on connaissait il y a dix ans, et c'est peut-être autour de la puissance des algorithmes qu'il faut aller chercher le noyau dur de cette définition. Même si le droit existant permet d'aborder beaucoup des questions qui se posent devant la très grande diversité des services que proposent les plateformes. On a bien compris que Google par exemple ne souhaitait pas se faire capturer dans ces filets car la diversité de ses activités trouve déjà d'autres réponses juridiques.

La deuxième réflexion tourne autour du principe de loyauté. C'est un principe qu'il faut arriver à forger. C'est une invitation à un travail collectif car, face à la révolution numérique, on pose très souvent la question de savoir s'il ne faut pas se débarrasser du droit. Le dire dans cette salle devrait faire tressaillir les invités à ce colloque, mais je constate qu'ils restent concentrés sur le sujet. Il faut donc continuer à réaliser ce travail collectif pour forger des principes, quand on a la conviction que le droit existant ne suffit pas, quelle que soit la qualité des applications proposées, l'attrait de leur interface utilisateur, la bienveillance lexicale dans laquelle nous baignons, même si l'autorégulation et les effets de réseau autour de l'autorégulation dont parlait Nicolas Colin sont extrêmement essentiels.

Je crois que le droit est encore ce qui permet tous les jours de rééquilibrer les rapports entre les faibles et les puissants. Il y a donc encore du travail au Conseil d'État et partout ailleurs dans la cité, car la révolution numérique ne fait que commencer.

Troisième table ronde

Le droit des États dans un univers transnational : quelle territorialité ?

La fréquente confrontation de systèmes juridiques différents qu'occasionne Internet est source d'une double difficulté pour les États. D'une part, la complexité des règles du droit international privé qui déterminent la loi applicable et la juridiction compétente, est source d'incertitudes. D'autre part, ces règles peuvent désigner des juridictions et des lois étrangères. Dès lors, l'État n'est plus totalement maître du jeu pour intervenir dans des domaines essentiels tels que la protection des données personnelles, la liberté d'expression ou la propriété.

Les enjeux stratégiques de la territorialité du fait d'Internet sont évidents. L'objectif est de trouver le bon équilibre entre le principe du pays de l'internaute et le principe du pays hébergeant le site Internet.

La table ronde devra vérifier si la préconisation du Conseil d'État consistant à promouvoir le principe du pays de l'internaute, non pour l'ensemble des règles juridiques applicables aux acteurs d'Internet, mais pour un socle de règles choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public, est pertinente. Elle s'interrogera, dans un contexte de législation européenne, sur la robustesse du concept de « loi de police » au sens du droit international privé.

Sommaire





Éléments de réflexion sur la territorialité du droit en matière numérique

Les difficultés de l'application territoriale du droit de l'Internet : la règle du pays de destination des contenus numériques ou la règle du pays d'origine de l'établissement émetteur ?

En rendant accessibles aux internautes de chaque pays les contenus et les services proposés dans le monde entier, Internet crée de très nombreux conflits entre les systèmes juridiques des différents États. L'affaire *LICRA et UEJF c/ Yahoo !*, relatif à la vente aux enchères d'objets nazis sur le site de ce moteur de recherche, l'a illustré avec éclat[142].

De nombreuses affaires ont, depuis lors, illustré la possibilité pour les juridictions d'un État de prononcer des décisions à l'encontre de sociétés établies dans d'autres États et exploitant des sites Internet. Au cours de l'année 2013, le tribunal de grande instance de Paris a ainsi enjoint à plusieurs moteurs de recherche établis aux États-Unis de *déréférencer* des sites proposant de manière massive des contenus méconnaissant le droit de la propriété intellectuelle ou des images portant atteinte à la vie privée d'une personnalité[143].

Cependant la fréquente confrontation de systèmes juridiques différents qu'occasionne Internet est source d'une double difficulté pour les États : d'une part, la complexité des règles de droit international privé, qui déterminent la loi applicable et la juridiction compétente, est source d'incertitudes ; d'autre part, ces règles peuvent désigner des juridictions et des lois étrangères. L'État est ainsi confronté à la possibilité que ses lois sur la protection des données personnelles, la liberté d'expression ou la propriété ne soient en définitive pas applicables à toutes les situations qu'il entend encadrer.

D'assez nombreuses décisions ont été rendues ces dernières années par la Cour de justice de l'Union européenne et la Cour de cassation, qui clarifient les solutions applicables aux situations fréquemment rencontrées sur Internet. De manière schématique, deux matières peuvent être distinguées : la matière pénale et quasi-

142 Par une ordonnance du 22 mai 2000, le juge des référés du tribunal de grande instance de Paris a ordonné à *Yahoo! Inc.*, la société-mère enregistrée aux États-Unis, « *de prendre toutes mesures de nature à dissuader et à rendre impossible toute consultation par un internaute appelant de France des sites et services litigieux dont le titre et/ou le contenu portent atteinte à l'ordre public interne, spécialement le site de vente d'objets nazis* ». La société *Yahoo!* a alors saisi la justice américaine pour lui demander de déclarer cette sentence non exécutable aux États-Unis, au motif qu'elle serait contraire au 1er amendement de la constitution américaine. Si le juge de première instance lui a donné gain de cause, la cour d'appel fédérale compétente l'a déboutée à deux reprises (Cour d'appel fédérale du 9e circuit, 23/8/2004 et 12/1/2006, *LICRA and UEJF v. Yahoo!*, n° 01-17424). Elle a notamment relevé que « *la France était en droit en tant que nation souveraine d'adopter des lois contre la distribution de propagande nazie, en réponse à sa terrible expérience des forces nazies durant la seconde guerre mondiale* » et que « *Yahoo! ne pouvait s'attendre à bénéficier du fait que ses contenus puissent être vus dans le monde entier tout en étant protégée des coûts qui en résultent* ».

143 TGI Paris, 6 novembre 2013, *Max Mosley c. Google Inc. et Google France*, RG 11/07970 – partie III « Sélection de jurisprudences ».

délictuelle, où prévaut le critère de l'activité « *dirigée* » vers un pays ; la matière contractuelle, où prévaut la volonté des parties. Toutefois, dans ce cas, il existe des exceptions, notamment lorsque l'une des parties est un consommateur, c'est-à-dire un non professionnel qui bénéficie alors de la possibilité de saisir la juridiction de son domicile et de l'application de sa loi nationale.

Un nécessaire équilibre entre principe du pays de l'internaute et principe du pays du site Internet

La territorialité sur Internet présente des enjeux de simplification et d'accessibilité du droit, mais aussi et surtout des enjeux stratégiques. L'objectif est de trouver le bon équilibre entre le principe du pays de l'internaute et le principe du pays du site Internet. Si le principe du *pays où est installé le site* prévaut, alors Internet est un facteur de mise en concurrence des systèmes juridiques, et les entreprises dont les systèmes juridiques sont les moins protecteurs peuvent en retirer un avantage concurrentiel ; en revanche, si le *principe du pays de l'internaute* s'applique, alors le lieu d'établissement de l'entreprise est sans incidence.

Il est difficilement envisageable que le principe du pays de l'internaute (application du droit de l'internaute qui utilise un service sur Internet) devienne une règle générale et absolue de détermination de la loi applicable sur Internet. Il y a un risque de *fragmentation* d'Internet, c'est-à-dire de différenciation des contenus accessibles selon les pays. Une telle orientation postulerait, en outre, que les acteurs français ou européens seront toujours voués à être sur Internet en situation de consommateurs et jamais de producteurs de services. Or, la France compte aussi des entreprises du numérique cherchant à développer leurs services à l'échelle mondiale ; pour elles, la sécurité juridique consiste à se voir appliquer les règles françaises partout dans le monde.

Définir un socle de règles applicables à tous les acteurs dirigeant leurs activités vers la France ou l'Union européenne

Le Conseil d'État préconise de promouvoir le *principe du pays de l'internaute* non pour l'ensemble des règles juridiques applicables aux acteurs d'Internet, mais *pour un socle de règles choisies en raison de leur importance* particulière dans la protection des droits fondamentaux ou de l'ordre public.

Selon les sujets, trois voies peuvent être envisagées pour faire prévaloir le principe du pays de destination : l'application des règles de droit commun du droit international privé (a) ; la qualification de loi de police (b) ; la coordination des législations nationales par un traité ou un acte de droit dérivé de l'Union européenne (c).

(a) Dans certains cas, l'application des règles de droit commun du droit international privé conduit à appliquer le principe du pays de destination. Ainsi, les lois pénales définissant les limites de la liberté d'expression revêtent une grande importance pour la sauvegarde des intérêts publics et doivent faire partie du socle. L'application des règles générales sur le champ d'application de la loi pénale permet d'aboutir au résultat recherché : en effet, le responsable du site Internet est responsable au titre de la loi pénale française si le site est dirigé vers le public français.

(b) Dans d'autres cas, il est en revanche nécessaire de s'écarter de la loi désignée par les règles générales de conflits de lois. Il en va notamment ainsi lorsque sont en cause des relations contractuelles, le droit international privé permettant aux parties de choisir la loi applicable au contrat, alors que le principe du socle est de faire prévaloir la loi nationale. Il faut donc rechercher des solutions dérogeant aux règles générales de conflits de lois. Le droit international privé reconnaît à cet égard deux possibilités : l'*exception d'ordre public* et la *loi de police*[144].

L'exception d'ordre public joue *a posteriori*, après examen de la loi étrangère désignée par la règle de conflit (par exemple, la loi déterminée par le contrat), dans l'hypothèse où une disposition de cette loi apparaît manifestement incompatible avec des valeurs essentielles de l'ordre juridique interne. La loi de police joue, quant à elle, *a priori*, avant tout examen de la règle de conflit. Il s'agit, selon les termes de l'article 9 du règlement « *Rome I* » sur la loi applicable aux obligations contractuelles, d'une « *disposition impérative dont le respect est jugé crucial par un pays pour la sauvegarde de ses intérêts publics, tels que son organisation politique, sociale ou économique, au point d'en exiger l'application à toute situation entrant dans son champ d'application* »[145]. La loi de police est plus appropriée que l'exception d'ordre public pour parvenir au résultat recherché : elle permet de faire prévaloir l'application de la règle nationale ou européenne en toute circonstance et de garantir ainsi une meilleure prévisibilité du droit applicable.

Les règles relatives à la protection des données personnelles ont vocation à entrer dans cette catégorie, dès lors qu'elles mettent en œuvre un droit garanti par la Charte des droits fondamentaux de l'Union européenne et que la protection des données personnelles est regardée aujourd'hui comme un enjeu de souveraineté. La qualification de loi de police étendrait à plusieurs égards leur champ d'application par rapport à ce que permettrait le jeu des règles de conflit. S'agissant des consommateurs, elle permettrait d'écarter l'application des lois étrangères désignées par les conditions générales d'utilisation des sites Internet, sans qu'il y ait besoin d'examiner si le site dirige son activité vers le pays de l'internaute (condition prévue par l'article 17.1 du règlement « *Rome I* »), ni si l'une ou l'autre des dispositions de la loi étrangère prive le consommateur d'une protection de son droit national (condition prévue par l'article 17.2). Quant aux contrats conclus entre entreprises, par exemple entre un responsable de traitement de données personnelles et un prestataire d'informatique en nuage, ils ne pourraient pas désigner une autre loi que la loi nationale (ou européenne si le règlement relatif à la protection des données personnelles est adopté). Combinée avec le large champ d'application territorial de la proposition de règlement, qui s'étend aux responsables de traitement établis hors de l'Union européenne lorsque leurs activités sont liées « *à l'offre de biens ou de services à ces personnes concernées dans l'Union* » ou « *à*

144 V. notamment M.-L. Niboyet et G. Geouffre de la Pradelle, *Droit international privé*, L.G.D.J, 2013.

145 L'article 16 du règlement « *Rome 2* » sur la loi applicable aux obligations non contractuelles prévoit une disposition similaire : « *Les dispositions du présent règlement ne portent pas atteinte à l'application des dispositions de la loi du for qui régissent impérativement la situation, quelle que soit la loi applicable à l'obligation non contractuelle* ».

l'observation de leur comportement » (article 3.2 de la proposition), la qualification de loi de police garantirait la protection des données personnelles des internautes selon les règles européennes, quel que soit le site visité, et empêcherait ces sites d'imposer l'application d'autres lois.

Un deuxième corps de règles devant s'imposer à tous les acteurs concernés a trait aux obligations de coopération avec les autorités judiciaires, ainsi qu'avec les autorités administratives procédant à des demandes de données de connexion dans le cadre du code de la sécurité intérieure. L'article 6 de la loi pour la confiance dans l'économie numérique, mis en œuvre par le décret n° 2011-219 du 25 février 2011, impose aux hébergeurs de transmettre à l'autorité judiciaire les données « *de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* », dans le but d'identifier les auteurs d'infractions pénales. L'article L. 246-1 du code de la sécurité intérieure permet également à l'autorité administrative, dans le cadre des finalités de protection de la sécurité nationale énumérées à l'article L. 241-3 du même code, de leur demander les mêmes données.

Or les grandes sociétés américaines ayant la qualité d'hébergeur, telles que *Facebook*, *Twitter* ou *Youtube*, ne s'estiment pas tenues par ces dispositions et répondent à leur guise aux demandes formulées par les autorités, selon des critères qui leur sont propres[146]. Ainsi, *Facebook* indique pour la France dans son *Government Requests Report* que « *nous répondons aux demandes valables concernant des affaires criminelles* » et que « *la légitimité de chacune des demandes que nous recevons est vérifiée, et nous rejetons les demandes trop vagues ou imprécises, ou nous demandons davantage de précisions sur celles-ci* » ; entre juillet et décembre 2013, *Facebook* n'a accédé qu'à 33,9 % des demandes qui lui ont été adressées. La loi actuelle est certes muette sur le champ d'application territorial de l'obligation de coopération des hébergeurs. Il paraît pourtant légitime que des sociétés qui dirigent leur activité vers la France, traitent les données d'internautes français et en retirent un bénéfice commercial, soient soumises aux mêmes obligations de coopération que les hébergeurs établis en France en matière pénale et de protection de la sécurité nationale. Rien ne leur interdit d'ailleurs, si elles estiment mal fondées les demandes qui leur sont adressées, de former des recours devant les juridictions judiciaires et administratives compétentes.

La qualification de loi de police est accordée par le juge. Toutefois, cette qualification est facilitée si le texte en cause définit explicitement son champ d'application territorial, prévoit qu'il s'applique nonobstant toute clause contractuelle contraire ou indique dans son exposé des motifs une intention de lui donner la portée d'une loi de police.

(c) La qualification de loi de police permet à un État, agissant de manière unilatérale, de faire prévaloir sa législation. Dans des matières où la qualification de loi de police n'est pas envisageable, l'application du principe du pays de destination ne peut résulter que d'un accord entre États, soit dans le cadre d'un traité, soit, pour les États membres de l'Union européenne, dans le cadre d'un acte de droit dérivé. En

146 V. notamment le rapport du groupe interministériel présidé par M. Robert sur la cybercriminalité.

matière de services de médias audiovisuels, le Gouvernement français a exprimé à plusieurs reprises son souhait de passer du principe du pays d'origine (aujourd'hui prévu par l'article 2 de la directive sur les services de médias audiovisuels, dite « *directive SMA* ») au principe du pays de destination. L'objectif poursuivi par cette proposition est que tous les services à destination du public français soient soumis au même régime juridique, notamment en matière de soutien à la production et d'exposition des œuvres françaises et européennes. Pour y parvenir, une modification de la directive SMA sera nécessaire.

En conclusion, il est proposé de redéfinir un socle de règles jouant un rôle décisif dans la protection des droits fondamentaux applicables à tous les acteurs dirigeant leur activité vers les internautes français ou européens, quel que soit leur lieu d'établissement. Ce socle comprendrait les catégories de règles suivantes :

- la *législation européenne* relative à la protection des données personnelles, qui serait qualifiée à cette fin de « loi de police » au sens du droit international privé ;
- l'*obligation de coopération des hébergeurs et des plateformes* avec les autorités administratives et judiciaires, prévue par l'article 6 de la loi pour la confiance dans l'économie numérique du 21 juin 2004 ;
- le *droit pénal*, qui est déjà applicable à l'ensemble des sites destinés au public français.





Présentation des intervenants

Présidente

Bénédicte Fauvarque-Cosson, *professeur à l'université de Paris II, présidente de la Société de législation comparée*

Professeur depuis 1995 (agrégation de droit privé et de sciences criminelles), Bénédicte Fauvarque-Cosson a étudié le droit en Angleterre et en France. Titulaire d'un doctorat en droit privé de l'Université Panthéon-Assas (1994), elle a été professeur à l'Université de Rouen, à l'Université de Paris V, puis à l'Université Panthéon-Assas (Paris II) à compter de 2002. Elle a été membre de l'Institut universitaire de France (2009-2014). Ses travaux portent sur le droit international privé, le droit comparé, le droit européen des contrats. Élue secrétaire générale de la Société de législation comparée en 2005, elle en assure la présidence depuis 2011. Elle est également cofondatrice et coprésidente de *Trans Europe Experts* (association d'experts juridiques européens, créée en 2009, dont les travaux portent notamment sur les données personnelles et le numérique), vice-présidente de l'Académie internationale de droit comparé et fut l'un des membres fondateurs de l'Institut européen du droit établi à Vienne. Depuis 2001 elle a participé à plusieurs réseaux de recherche internationaux et européens en droit des contrats. Elle est directrice scientifique du *Recueil Dalloz*.

Intervenants

Édouard Geffray *, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL)*

Édouard Geffray, maître des requêtes au Conseil d'État, était auparavant directeur des Affaires juridiques internationales et de l'expertise de la CNIL. Précédemment, il a été successivement rapporteur à la dixième sous-section du contentieux du Conseil d'État de 2005 à 2008, responsable du centre de documentation et de recherches juridiques – service chargé d'effectuer les recherches juridiques pour les membres du Conseil d'État – en 2008 et rapporteur public à la troisième sous-section du contentieux de décembre 2008 à janvier 2012. Ancien élève de l'ENA, Édouard Geffray est diplômé de l'Institut d'études politiques de Paris et titulaire d'une maîtrise d'histoire.

Marc Mossé, *directeur des affaires juridiques et publiques, membre du comité de direction de Microsoft France*

Marc Mossé a créé et dirige le laboratoire d'idées de Microsoft France : « RSLN - Regards sur le Numérique ». Ancien collaborateur parlementaire de Robert Badinter, il a exercé comme avocat jusqu'en 2003 en intervenant particulièrement en droit des nouvelles technologies et de la propriété intellectuelle, en droit public et s'est investi pour la défense des libertés publiques et notamment en contentieux

constitutionnel. Vice-président de l'Association française des juristes d'entreprise (AFJE), il est actuellement secrétaire général de l'Union des fabricants et siège au Conseil supérieur de la propriété littéraire et artistique. Maître de Conférences à Science Po Paris dans le cadre du Master affaires publiques, il a créé un séminaire sur la responsabilité sociale des entreprises. Il est aussi vice-président du *think tank* Renaissance Numérique et participe à l'initiative *Respect Zone*. Ancien Secrétaire de la Conférence du stage des avocats au Conseil d'État et à la Cour de Cassation, il est titulaire d'un DEA de droit public et d'un DEA de droit européen des Universités de Paris I et Paris V.

Winston Maxwell, *avocat associé à Hogan Lovells*

Diplômé en droit de l'université Cornell aux États-Unis, Winston Maxwell est l'un des principaux avocats spécialisés en France dans les technologies, les médias, les télécommunications et la protection des données. Dans le cadre de ses activités liées à la protection des données personnelles et de la vie privée, Maître Maxwell a notamment été auditionné par la CNIL et plusieurs commissions parlementaires en France sur la réforme de la législation sur les données personnelles. Dans le domaine des télécommunications et d'Internet, Maître Maxwell est le coauteur d'un rapport remis à la Commission européenne, et d'un rapport pour l'Autorité de régulation des communications électroniques et des postes (ARCEP). En 2014, il a été nommé membre de la commission parlementaire de réflexion sur le droit et les libertés à l'âge du numérique. Il est par ailleurs coprésident du comité «économie numérique» de la chambre de commerce américaine en France, membre de l'*International Association of Privacy Professionals* et membre de l'*International Association of Entertainment Lawyers*. Il est l'auteur de nombreux articles sur le numérique et la protection des droits fondamentaux.

Alain Strowel, *professeur à l'université Saint-Louis (Bruxelles) et à l'université catholique de Louvain*

Alain Strowel est professeur ordinaire à l'Université Saint-Louis (Bruxelles) et à l'Université catholique de Louvain. Il enseigne également dans divers masters spécialisés en Europe (KULeuven et *Munich Intellectual Property Law Centre*). Ses cours couvrent notamment le droit d'auteur, l'interface entre la propriété intellectuelle et le droit de la concurrence, le droit des médias. Alain Strowel est avocat au barreau de Bruxelles depuis 1988. Sa pratique porte sur le droit d'auteur numérique et le droit de l'Internet. Il est tiers-décideur pour l'Organisation mondiale de la propriété intellectuelle et pour le système alternatif de règlement des conflits en matière de noms de domaine « .be ». Il est l'auteur de plus de deux cents articles et de quelques livres dont *Quand Google défie le droit* (De Boeck-Larcier, 2011). Il a coordonné plusieurs recueils de contributions parmi lesquels: *Peer-to-Peer File Sharing and Secondary Liability in Copyright Law* (Edward Elgar, 2009), *Le téléchargement d'œuvres sur Internet* (Larcier, 2012, avec C. Doutrelepont et Fr. Dubuisson), *Net Neutrality in Europe - La neutralité de l'Internet en Europe*, (Bruylant, 2013), *Droit, Economie, Valeurs*, (Larcier, 2014, avec. A. Autenne et V. Cassiers).

Actes – Le droit des États dans un univers transnational: quelle territorialité?

Bénédicte Fauvarque-Cosson
Professeur à l'université Panthéon-Assas,
présidente de la Société de législation comparée

Je remercie les organisateurs de ce colloque de m'avoir invitée à présider cette table ronde, composée des intervenants suivants : Édouard Geffray, secrétaire général de la CNIL et maître des requêtes au Conseil d'État ; Winston Maxwell, avocat associé au cabinet *Hogan Lovells*, coauteur d'un rapport et de très nombreux écrits dont un article publié dans l'étude annuelle 2014 du Conseil d'État sur la jurisprudence américaine en matière de liberté d'expression sur Internet[147] ; Marc Mossé, directeur des affaires juridiques et publiques, membre du comité de direction de *Microsoft France* ; et Alain Strowel, professeur à l'université Saint-Louis de Bruxelles et à l'université catholique de Louvain, également avocat au barreau de Bruxelles.

Les organisateurs de ce colloque m'ont demandé, en ma qualité d'universitaire, de faire œuvre de pédagogie et de présenter les grands principes qui s'appliquent en droit international privé, discipline qui permet de trancher les conflits de lois ainsi que les conflits de juridictions. Toute la difficulté vient de ce que le numérique est un phénomène déterritorialisé. On cherche à bâtir un cadre non étatique au-delà des États et en dehors d'eux.

C'est pourquoi, je commencerai par évoquer le rêve du grand projet d'une *lex electronica* fondée sur l'idée que l'Internet pourrait faire l'objet d'un système d'autorégulation supranational, comme au Moyen Âge la loi des marchands, la *lex mercatoria*. Dans les années 1990, on se mit à imaginer de nouvelles règles pour réguler le cyberespace qui défie les frontières territoriales, incluses dans une *lex electronica*. Cela a assez bien fonctionné pour les questions liées à la gouvernance de l'Internet, comme par exemple la création de l'ICANN[148]. Mais, en ce qui concerne la protection des droits fondamentaux, cette idée est assez utopique. Ce serait une erreur de croire que la régulation du cyberespace possède une normativité véritablement internationale, naturellement internationale.

Le risque serait alors de se laisser dicter nos valeurs et nos lois par d'autres acteurs, qui ne sont pas nécessairement des juristes. Dans un article publié en l'an 2000, intitulé : « *Code is law* » (en français, *le code fait loi*)[149], Lawrence Lessig explique que, finalement, tout passe non par les normes juridiques mais par l'architecture

147 V. Conseil d'État, étude annuelle 2014, *Le numérique et les droits fondamentaux*, La documentation Française, p. 393 à 406.

148 *Internet Corporation for Assigned Names and Numbers* (ICANN) ; en français : *Société pour l'attribution des noms de domaine et des numéros sur Internet*. L'ICANN est un organisme à but non lucratif responsable de la sécurité, de la stabilité et de la coordination mondiale du système d'identificateurs uniques de l'Internet.

149 L/ Lessig, « Code is Law », *Harvard Magazine*, 2000.

technique des plateformes que nous utilisons et qui crée *de facto* une forme de régulation supranationale. Si la technologie précède le droit, elle ne peut pas s'y substituer. Alors, comment assurer la protection des droits individuels dans cet univers dématérialisé et internationalisé ? Quelle place reste-t-il pour nos raisonnements habituels ? M. le vice-président Sauvé nous a appelé à faire œuvre révolutionnaire et à faire preuve d'audace pour remettre en cause les paradigmes auxquels nous sommes habitués : un monde divisé en États souverains avec des lois nationales ; et c'est pourquoi, lorsqu'il y a un élément d'extranéité et qu'il faut trancher un conflit de lois, on utilise la règle de conflit de lois qui désigne indifféremment la loi française ou une loi étrangère. Traditionnellement, cette règle est un procédé bilatéral neutre qui se préoccupe d'une justice du rattachement et recherche l'application de la loi qui présente les liens les plus étroits avec l'affaire.

L'étude annuelle 2014 du Conseil d'État insiste sur l'importance de promouvoir un modèle européen fort, humaniste, respectueux des personnes et qui garantit un certain équilibre avec d'autres libertés fondamentales. Les valeurs à défendre sont affirmées par l'article 8 de la Convention européenne des droits de l'Homme[150], par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne[151], par l'article 16 du TFUE[152], par la jurisprudence de la Cour de justice de l'Union européenne et, tout récemment, par la déclaration commune du groupe de travail « article 29 »[153] adoptée lors de sa séance plénière à Paris le 25 novembre 2014 qui réaffirme les valeurs communes de l'Europe et propose des actions concrètes aux fins d'élaborer un cadre éthique européen[154].

D'un côté, il faut protéger l'individu et, de l'autre, permettre le développement du marché du numérique, priorité de l'Union européenne, tout en garantissant la confiance des internautes et en respectant les consommateurs et l'industrie. Tout cela fait partie de ce que l'on appellerait, en droit international privé, « *l'ordre public européen* ». Cet ordre public n'est pas figé, nous avons dans cette matière un principe d'actualité de l'ordre public. Ainsi, il fut un temps où nous écartions les

150 « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* », Convention européenne des droits de l'Homme, art. 8 § 1.

151 « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* », Charte des droits fondamentaux de l'Union européenne, art. 7 (Respect de la vie privée et familiale) ; « *1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante* », Charte des droits fondamentaux de l'Union européenne, art. 8 (Protection des données à caractère personnel).

152 « *Toute personne a droit à la protection des données à caractère personnel la concernant* », Traité sur le fonctionnement de l'Union européenne (TFUE), art. 16 § 1.

153 L'article 29 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, a institué le *groupe de travail « article 29 »* (aussi appelé G29) rassemblant les représentants de chaque autorité indépendante de protection des données nationales. Cette organisation, qui réunit l'ensemble des CNIL européennes, a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays hors Union européenne et de conseiller la Commission européenne sur tout projet ayant une incidence sur la protection des données et des libertés des personnes. Le G 29 se réunit à Bruxelles en séance plénière tous les deux mois environ.

154 V. le site de la CNIL http://www.cnil.fr/linstitution/international/g29/edgf14/

lois étrangères qui autorisaient le divorce, puis vint le temps où nous avons écarté les lois étrangères qui… interdisaient le divorce. De la même façon, les valeurs qui font partie de cet ordre public européen en matière de données personnelles pourraient changer, comme l'ont montré par exemple les débats précédents avec Me Alain Bensoussan expliquant qu'il fallait favoriser la propriété et le Conseil d'État qui privilégie l'autodétermination informationnelle. Par ailleurs, il existe une autre difficulté : plus les droits fondamentaux se développent, plus ils vont entrer en conflit les uns avec les autres. Et le droit international privé qui, jusqu'à présent, devait résoudre des conflits de lois étatiques, se trouve aujourd'hui amené à résoudre des conflits de droits fondamentaux : par exemple, le droit à l'oubli d'un côté, la liberté d'expression de l'autre.

Alors, comment faire pour savoir à quelle loi soumettre la situation en l'absence d'une grande réglementation internationale ? Quel juge saisir, et dans quelles conditions reconnaître et donner effet à une décision prononcée par exemple en France mais dont l'effet sera demandé aux États-Unis ?

En pratique les choses ne sont pas simples, car les grandes entreprises de l'Internet sont presque toutes établies aux États-Unis et les internautes, eux, sont situés dans le monde entier, notamment en Europe. On pourrait songer à prévoir l'application de *la loi de résidence* de l'internaute, mais cela reviendrait à demander à un site de se conformer à toutes les lois de tous les pays du monde. L'étude annuelle 2014 du Conseil d'État écarte cette application systématique de la loi de la résidence de l'internaute car elle présente le risque d'augmenter la fragmentation de l'Internet.

On pourrait alors songer à se tourner vers la loi du pays d'origine du site concerné, mais cela risquerait d'être la porte ouverte à toutes sortes de fraudes ou d'attitudes opportunistes. On pourrait encore songer en matière contractuelle à se contenter de la loi d'autonomie, c'est-à-dire la loi choisie par les parties, comme c'est le cas actuellement pour de nombreux contrats, notamment en matière d'informatique en nuage (*cloud computing*)[155], avec pour inconvénient que les grandes entreprises cherchent à imposer le droit applicable et le juge compétent.

De ces éléments découle la proposition n°43 de l'étude annuelle 2014 du Conseil d'État[156], proposition dont nous allons débattre : définir un « *socle de règles impératives* » pour tous les services dirigés vers l'Union européenne ou la France, quel que soit leur lieu d'établissement.

Comment rendre ce socle de règles applicable ? D'abord, par l'application des règles classiques du droit international privé. En droit pénal, cela fonctionne

155 L'informatique en nuage, en anglais « *cloud computing* », est l'accès à la demande et en libre service, à travers un réseau de télécommunication, généralement Internet, à des ressources informatiques partagées sur des serveurs distants.

156 « *Définir un socle de règles applicables à tous les services dirigés vers l'Union européenne ou la France, (selon que la règle est européenne ou nationale), quel que soit leur lieu d'établissement. Ce socle comprendrait : la législation européenne relative à la protection des données personnelles, qui serait qualifiée à cette fin de* « loi de police » *au sens du droit international privé ; l'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judicaires, prévue à l'article 6 de la loi pour la confiance dans l'économie numérique* [loi n° 2004-575 du 21 juin 2004]*, dont le champ d'application territorial serait explicité ; et le droit pénal, qui est déjà applicable à l'ensemble des sites destinés au public français* ».

assez bien puisque ces règles vont conduire au principe du pays de destination : il y a donc une sorte de territorialité directionnelle, si bien que l'on arrive au but poursuivi. Mais ce n'est pas le cas dans les autres domaines. L'étude annuelle 2014 du Conseil d'État propose alors de s'écarter des règles habituelles de conflit de lois lorsqu'elles sont inadaptées : soit pour recourir à *l'exception d'ordre public*, c'est-à-dire vérifier que la règle étrangère désignée respecte les valeurs fondamentales européennes, ce qui suppose d'abord de la rendre applicable, puis de l'examiner et enfin de l'écarter si ce n'est pas le cas ; soit, autre technique, pour utiliser la méthode des *lois de police*.

Les lois de police sont des lois d'application immédiate qui vont s'appliquer *a priori* sans le détour par la règle du conflit de lois. Cette méthode unilatérale, bien sûr, ne respecte pas une égalité parfaite entre la loi du for[157] et les lois étrangères. Cette solution est proposée par le Conseil d'État dans son étude annuelle 2014 notamment pour les règles relatives à la protection des données personnelles. Il sera intéressant de voir si la proposition de règlement, qui a redéfini le champ d'application territorial de son domaine, va dans ce sens et si le nouvel article 3 consacre cette idée d'une application immédiate des dispositions sur les données, à titre de loi de police.

On constate également que la définition de la loi de police, qui est donnée par le règlement « *Rome I* »[158] et remonte à une définition ancienne de Francescakis, un auteur grec spécialiste de droit international privé[159], a été reprise dans la déclaration commune du 25 novembre 2014 des autorités européennes de protection des données réunies au sein du groupe de travail « article 29 ». En effet, au sein de cette déclaration, l'article 14 précise que « *Les règles de protection des données de l'Union sont nécessaires à la sauvegarde de la situation politique, sociale et économique de l'Union et de ceux qui sont soumis à la législation de l'Union* [– on est bien ici dans la notion de droit de police ! –]. *Elles doivent être considérées comme des principes internationaux impératifs en droit international public et privé. Des lois étrangères ou des accords internationaux ne peuvent leur passer outre et les organisations ne peuvent y déroger par contrat* »[160]. On peut noter que si les anglo-américains utilisent davantage l'expression de règle internationale impérative (en anglais « *international mandatory rule* ») plutôt que celle de loi de police, on reste néanmoins vraiment dans l'idée de loi de police.

157 La loi du for (en latin, *lex fori*) est une notion propre au droit international privé, qui signifie : la loi (*lex*) applicable au lieu (*forum*) où se trouve installé le tribunal devant lequel l'affaire a été portée. Lorsqu'un juge est saisi d'une affaire qui présente un caractère international, il doit s'interroger sur la loi applicable à cette affaire. Dans certaines hypothèses, ce sera la *lex fori* qui s'appliquera. Traditionnellement, la *lex fori* régit les questions de procédure, quelle que soit la *lex causae* (la loi, telle que désignée par les règles de conflits de lois, qui régit le fond de l'affaire).

158 Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles, dit « *Rome I* ».

159 Phocion Francescakis (1910-1992), docteur en droit spécialisé en droit international privé, a été directeur de recherche honoraire au CNRS, professeur à l'Institut de droit comparé de l'université de Paris et à l'université de Thessalonique.

160 Déclaration commune du 25 novembre 2014 des autorités européennes de protection des données réunies au sein du G29, chapitre sur « l'influence européenne », art. 14.

Enfin, la troisième voie qui peut se dégager, c'est de parvenir à conclure des accords entre États pour éventuellement favoriser l'application du principe du pays de destination, donc la voie de la coopération.

Telles sont les voies possibles pour donner une portée extraterritoriale à notre droit. Reste la question de la loi étrangère qui, elle, veut imposer sa portée extraterritoriale ; et il serait intéressant en la matière de voir comment font les Américains à qui l'on reproche souvent – non sans raison – de vouloir donner, dans beaucoup de domaines, une portée extraterritoriale à leur droit, notamment pour favoriser leurs entreprises.

Pour lancer les interventions, je donne la parole à Édouard Geffray pour traiter des aspects juridiques et pratiques de la territorialité du droit en matière de protection des données personnelles. Puis, Me Maxwell s'intéressera aux États-Unis et à la manière dont la primauté donnée dans ce pays à la liberté d'expression peut générer certaines incompréhensions.

Édouard Geffray

Secrétaire général de la CNIL

La territorialité pose la question de la souveraineté juridique, c'est-à-dire de la capacité d'appliquer notre droit – national ou européen – à la fois sur notre territoire et sur nos résidents. Il y a deux phénomènes qui, aujourd'hui, viennent tempérer cette souveraineté. Le premier, c'est que le numérique est un phénomène qui non seulement est déterritorialisé mais également dématérialisé. Il est donc très difficile de saisir la nature de l'activité numérique pour lui appliquer une norme juridique. Le second phénomène, c'est que nous sommes dans un environnement juridique marqué par le poids croissant de législations extraterritoriales de la part de pays tiers à l'Union européenne.

Le champ des données personnelles se trouve à la croisée des chemins de ces évolutions puisque l'on est, à la fois, sur la protection d'un droit fondamental[161] dont il est important d'assurer la continuité au-delà des frontières ; sur une matière qui est par nature volatile : la circulation des données personnelles ; et en même temps sur un secteur qui intéresse les États et les entreprises, puisque qu'il fait l'objet de nombreuses législations qui visent, en fait, à capter les données personnelles des résidents européens.

Généralement, quand on parle de ces défis, on me pose la question : « *que peut-on faire* » ? La réponse est très claire. Elle est donnée notamment par l'étude annuelle 2014 du Conseil d'État et par les travaux de la CNIL et du groupe de travail « article 29 » sur la protection des données qui réunit les autorités de protection des données personnelles de toute l'Union européenne : il existe des solutions qui sont juridiquement possibles, pratiquement envisageables et, en tout état de cause, nécessaires.

161 L'article 8 de la Charte des droits fondamentaux de l'Union européenne consacre ainsi la protection des données à caractère personnel comme une liberté fondamentale.

1. Avant d'en venir à ces solutions, je souhaiterais faire un rappel sur la réglementation actuelle européenne en matière de protection des données personnelles.

Il s'agit de la fameuse directive de 1995 sur la protection des données[162], ainsi que des droits nationaux qui en sont issus par voie de transposition. Ce qui est intéressant en termes d'applicabilité territoriale, c'est que nous sommes face à un droit fondamental, au sens de l'article 8 de la Charte des droits fondamentaux de l'Union européenne, c'est-à-dire un *droit liberté*. Les textes qui régissent aujourd'hui la protection des données personnelles prévoient un critère d'application fondé sur l'existence de ce que l'on appelle le « *responsable de traitement* », à savoir l'entreprise qui traite les données, ou sur la localisation de ses moyens de collecte. Ainsi, le droit européen s'applique à condition que l'établissement soit basé en Europe ou que ses moyens de collecte soient eux-mêmes basés en Europe.

Le terme *moyen de collecte* est appréhendé par les CNIL européennes dans un sens assez large. C'est typiquement le cas, par exemple, d'un « *témoin de connexion* » (« *cookie* »)[163] installé sur l'ordinateur de l'internaute, qui envoie une information à un tiers. Quand il s'agit d'un fichier texte installé sur un ordinateur situé en France, les moyens de collecte étant en France, le droit européen s'applique.

Mais on voit bien que ces règles soulèvent des questions entre, d'un côté, un droit fondamental attaché à la personne et, de l'autre, une logique conçue par rapport à l'entité qui exerce le traitement.

Pour autant, cela n'interdit pas une forme de *contagion* de la protection du citoyen dans une logique extraterritoriale.

Prenons deux exemples concrets. Le premier exemple est celui du déréférencement. La CJUE, dans son arrêt du 13 mai 2014 *Google Spain*[164], a jugé que le droit européen s'applique dès lors que l'un des établissements en Europe participe à un traitement mis en œuvre plus généralement par des entités installées ailleurs qu'en Europe, en l'occurrence le moteur de recherche *Google*. Dès lors qu'une entité implantée en France participe à la publicité ciblée sur les services mis en œuvre par *Google Inc.*, le droit européen s'applique. La CJUE en déduit que le droit à l'effacement ou droit d'opposition s'appliquent, ce qui, quand on fait masse des deux, dans le cadre d'un moteur de recherche, donne un droit au déréférencement. Ce droit est un droit à la *décorrélation* entre un nom et un résultat qui apparaît dans la page du moteur de recherche.

Reste alors à clarifier concrètement la portée de ce droit : un résultat relatif à un résident en France doit-il être déréférencé sur *google.fr* ou également sur les

162 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.

163 Le « *témoin de connexion* » est l'équivalent d'un petit fichier texte stocké sur l'ordinateur de l'internaute. Il permet aux développeurs de sites Internet de conserver les données de connexion des utilisateurs pour faciliter leur navigation et leur offrir certaines fonctionnalités (authentification, etc.). Ces fichiers de texte, bien que n'étant ni exécutables, ni logiciels espions, ni virus, sont associés à un identifiant unique, propre au terminal utilisateur – donc à la personne qui l'utilise – et permettent notamment d'assurer le « *traçage* » de la navigation d'un internaute entre plusieurs sites.

164 CJUE, aff. C-131/12, 13 mai 2014, *Google Spain et Google*.

autres terminaisons comme *google.com* ? Juridiquement, la réponse nous semble claire : cela doit également s'appliquer à *google.com*, à la fois pour des raisons juridiques (j'ai un droit à l'égard du *traitement* de mes données, quelle que soit la modalité d'entrée sur le réseau) et pour des raisons pratiques (la protection du droit européen, attachée à la donnée, doit me suivre partout). Un exemple très révélateur de cette réalité : lorsque l'internaute français saisit « *google.com* » dans la barre d'adresse de son navigateur, il se retrouve spontanément en .fr ; en revanche, en cliquant en bas de la page d'accueil, il peut utiliser le moteur de recherche en .com, comme il peut utiliser d'autres terminaisons (.uk, .de, etc.). Cette question reste encore un point en débat, car tous les moteurs de recherche ne considèrent pas les choses de la même façon.

Le second exemple concerne le transfert international de donnés personnelles. En principe, il est interdit de transférer les données personnelles des individus en dehors de l'Union européenne, sauf dans des cas très précis prévus par les textes, notamment s'il existe une « *adéquation* », c'est-à-dire si le pays de destination a un standard de protection qui est adéquat par rapport au nôtre, ou bien s'il existe un dispositif de nature contractuelle qui permette de garantir le même niveau de protection quel que soit le devenir de la donnée. C'est par exemple le cas des règles internes d'entreprise (« *binding corporate rules* »)[165] que les CNIL européennes ont inventées. Cet outil permet de faire librement circuler les données à l'intérieur d'un groupe, quelle que soit la localisation de ses filiales dans le monde, si ce groupe applique ces règles, c'est-à-dire s'il s'engage à respecter le standard européen de protection des données.

Il y a donc un effet extraterritorial, mais qui est exclusivement destiné à garantir la protection des données du résident européen – c'est-à-dire la protection d'un droit fondamental –, contrairement à des législations extraterritoriales qui visent à avoir des effets sur les résidents de pays tiers.

2. L'enjeu est dès lors d'assurer la protection des données personnelles du résident européen, à la fois « positivement » mais aussi face à de nouveaux types de collecte massive. C'est l'un des objectifs du règlement européen.

Il existe en effet un enjeu majeur quant à la protection du droit des personnes vis-à-vis des législations extraterritoriales de pays tiers, qui n'ont pas pour objet d'étendre la protection des données à caractère personnel de leurs résidents, mais de capter les données personnelles des personnes non résidentes. Il existe un certain nombre de législations, parfaitement légales du point de vue du droit de leur pays d'origine, qui se traduisent par de la captation de données.

Si je prends l'exemple des États-Unis, qui n'est pas le seul, vous avez : en matière d'ordre public les effets du *Patriot Act* ; en matière bancaire l'effet de ce qu'on appelle le FATCA[166] qui oblige les banques européennes à transmettre des données aux autorités américaines lorsqu'il y a une « *présomption d'américanité* » de leur

165 Les règles internes d'entreprise ou « *Binding Corporate Rules* » (BCR) désignent un code de conduite interne qui définit la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne.

166 *Foreign Account Tax Compliance Act*.

client ; la loi Sabanes-Oxley[167] sur tout ce qui concerne la comptabilité d'entreprise, etc. Nous avons donc aujourd'hui des législations en tuyaux d'orgue, venues de pays tiers et à vocation extraterritoriale, qui peuvent conduire à la captation plus ou moins massives de données personnelles.

Quelle réponse apporter à cela ? La première chose, c'est que dans cet univers numérique dématérialisé, il faut à mon sens constater et admettre une certaine forme « *d'extraterritorialité croisée* ». Il est difficile d'imaginer un monde numérique sans quelques effets extraterritoriaux des législations, puisque le numérique s'affranchit partiellement des frontières. Simplement, il faut faire en sorte à la fois de protéger les droits fondamentaux de nos résidents et d'opposer des garde-fous à des législations qui seraient par trop intrusives.

De ce point de vue, le triptyque juridique suivant peut être utilement envisagé :

Le premier élément a trait à l'applicabilité du droit européen, et plus particulièrement au critère dit du « *ciblage* ». Le projet de règlement européen sur la protection des données personnelles, qui remplacera bientôt la loi française de 1978 et la directive européenne de 1995, a en effet pour principale nouveauté de poser que le droit européen s'applique dès lors qu'un résident européen est « *ciblé* » par un traitement de données à caractère personnel, quel que soit le lieu d'implantation du « *responsable du traitement* ».

Le deuxième élément touche à la hiérarchie des normes en droit international, et à l'application systématique d'une législation européenne dont on considère qu'elle est si fondamentale et indissociable de notre conception de l'État de droit qu'elle doit s'imposer. C'est évidemment la question de la loi de police, qui est une nécessité que les CNIL européennes partagent et qu'elles ont rappelée dans leur déclaration commune du 25 novembre 2014. Cela qui signifie que d'hypothétiques accords internationaux entre l'Union et des pays tiers ne peuvent pas avoir pour effet d'y déroger.

Le troisième et dernier élément concerne les modalités d'encadrement des collectes de données par des autorités publiques de pays tiers. À cet égard, il existe une disposition très intéressante du règlement européen, qui est l'actuel article 43-a (dans la version issue du Parlement européen), qui consiste à dire qu'il faut soumettre la demande d'autorités publiques des pays tiers voulant l'accès à des données personnelles de résidents européens à un accord des autorités publiques européennes. L'article 43 prévoit que ces autorités sont les CNIL européennes[168]. Aujourd'hui, il existe une asymétrie juridique : d'un côté, il existe des lois dans des pays tiers qui imposent aux entreprises de livrer des données personnelles sous peine de sanctions lourdes ; de l'autre, il n'existe pas de disposition européenne qui permette d'équilibrer la situation. C'est pourquoi une obligation, comme celle posée par l'article 43 précédemment cité, qui peut conduire à une sanction en cas

167 Loi de 2002 imposant de nouvelles règles sur la comptabilité et la transparence financière.

168 V. 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 (règlement général sur la protection des données)*, proposition COM(2012)0011, procédure 2012/0011(COD).

de non respect, permet de créer une forme de conflit de lois obligeant *de facto* à un accord transnational qui garantisse le caractère ciblé, proportionné et adéquat de l'accès aux données personnelles. À ce moment-là, on retrouve des critères qui sont les nôtres, même s'ils sont activés au bénéfice de pays tiers.

En conclusion, vous avez sans doute compris que je suis assez convaincu que le droit européen est encore souverain et peut s'appliquer, et que la protection des données personnelles en est une illustration essentielle. Elle l'est d'autant plus qu'elle représente à mon sens un « droit d'infrastructure » : dans le numérique, l'atome de base est la donnée personnelle. Elle conditionne la liberté de pensée, la liberté d'expression, dans certains cas la liberté de vote ; elle conditionne parfois la liberté d'aller et venir. Toutes ces libertés impliquent une protection adaptée qui ne s'efface pas lorsque les données passent les frontières. Cela est techniquement possible, juridiquement nécessaire et philosophiquement consubstantiel à ce que nous sommes.

Bénédicte Fauvarque-Cosson
Professeur à l'université Panthéon-Assas,
présidente de la Société de législation comparée

Merci pour ces propos précis et fermes qui représentent la vision européenne. Je me tourne vers M. Maxwell qui, tout en exerçant en France, connaît sans doute beaucoup mieux que nous la manière dont les Américains appréhendent cette question. Est-ce que la protection des données personnelles est perçue de la même manière en Europe et aux États-Unis ? N'y a-t-il pas d'autres droits fondamentaux, peut-être encore plus importants ?

Winston Maxwell
Avocat associé à Hogan Lovells

La question de la protection des données personnelles aux États-Unis est un sujet important. Je vais cependant me concentrer aujourd'hui sur la liberté d'expression qui entre souvent en frottement avec les politiques européennes de contenu, notamment pour ce qui concerne le droit à l'oubli. Je vais ainsi vous exposer brièvement les dispositions du premier amendement et ses conséquences au sujet de l'expression sur Internet, pour ensuite parler de la territorialité.

1. Le premier amendement est très similaire au principe européen sur la liberté d'expression[169], il interdit toute restriction de la liberté d'expression *par l'État*. J'insiste sur la formule « *par l'État* » car, dès le début, il existe dans la philosophie américaine une grande méfiance envers l'État ; c'est le sens de notre Déclaration des droits (« *Bill of Rights* »)[170]. La liberté d'expression aux États-Unis comme en

169 « *Le Congrès ne fera aucune loi relative à l'établissement d'une religion, ou à l'interdiction de son libre exercice ; ou pour limiter la liberté d'expression, de la presse ou le droit des citoyens de se réunir pacifiquement ou d'adresser au Gouvernement des pétitions pour obtenir réparations des torts subis* », 1er amendement de la Constitution des États-Unis d'Amérique.

170 La Déclaration des droits (« *Bill of Rights* ») est l'ensemble constitué des dix premiers amendements à la Constitution des États-Unis d'Amérique.

Europe n'est pas absolue. Il y a des cas où les propos diffamatoires, les publicités mensongères et les menaces sont interdits. Pour appliquer ce grand principe de liberté d'expression, les tribunaux utilisent une approche qui ne s'appelle pas test de proportionnalité mais « *balancing test* ».

Mais parce que les valeurs sociétales évoluent avec le temps, l'appréciation de la liberté d'expression dépend également de l'époque. Au moment de la Seconde Guerre mondiale, en 1940, le Congrès a adopté une loi qui interdisait tout propos incitant le renversement du Gouvernement des États-Unis et qui obligeait tout résidant américain étranger à s'inscrire auprès des autorités. Cette loi qui s'appelle le *Smith Act*[171] a été utilisée après la guerre pour poursuivre les communistes dans la période de Mc Carthy. Elle a été déclarée inconstitutionnelle à la fin des années 1950. En même temps, il y avait une loi de l'État de l'Illinois qui était très similaire à la loi sur la presse en France qui interdisait la publication de propos incitant à la haine raciale, et la Cour suprême a validé cette loi comme étant parfaitement conforme avec la liberté d'expression.

Avec le temps, les choses ont évolué. En 1992, la Cour suprême des États-Unis a pris une décision très importante[172] qui a invalidé un arrêté municipal qui interdisait toute manifestation néonazie ou du Klu Klux Klan et interdisait également l'utilisation de croix gammées. La Cour suprême a ainsi changé complètement de cap et a interdit à l'État de faire des choix idéologiques, avec comme principe qu'il faut permettre l'expression de toutes les idées, même les plus affreuses. En revanche, il reste possible à l'État de réguler les circonstances d'expression de ces idées. Par exemple, un arrêté municipal pourrait interdire toute manifestation publique après vingt-deux heures ou délimiter le périmètre de la manifestation, à condition que cette régulation reste neutre par rapport au contenu mais vise juste ses modalités d'application. C'est ce que l'on appelle les *restrictions horaire, lieu et manière* (en anglais, « *time, place and manner restrictions* »).

Ce revirement de la jurisprudence traduit une méfiance extrême vis-à-vis de l'État comme régulateur des points de vue et du marché des idées. C'est un aspect culturel important des Américains par rapport à l'approche européenne. Pour les Américains, l'État est peut être le plus mal placé pour choisir ce qui est une bonne ou une mauvaise idée. Car, si l'on s'engage dans cette voie, l'État pourrait en profiter pour favoriser des idées qui assurent le *statu quo* politique, avec le risque de conflit d'intérêt de la part des décideurs politiques. Certains affirment même que l'État représente le monopole le plus dangereux ; cette philosophie est omniprésente dans la jurisprudence sur la liberté d'expression aux États-Unis.

Le deuxième grand cas s'est produit en 1996 avec la loi sur la décence dans les communications (« *Communication Decency Act* »). Au début de l'Internet, le Congrès américain avait voté une loi imposant aux éditeurs de site de s'assurer que les contenus indécents ou sexuellement explicites ne soient pas accessibles aux mineurs. Loi que le ministre de la Justice avait soutenue devant la Cour suprême, en arguant du fait qu'une telle régulation existait déjà pour la télévision. Mais la

171 *The Alien Registration Act of 1940 (Smith Act), 76th United States Congress, 3rd session, ch. 439, 54 Stat. 670, 18 U.S.C. § 2385*.

172 *U.S. Supreme Court*, 22 juin 1992, *R.A.V. vs St. Paul*, n° 90-7675.

Cour suprême a refusé de valider cette loi[173] en expliquant qu'Internet n'est pas comme la télévision, un service audiovisuel intrusif où il existe une rareté des fréquences, mais est similaire à la distribution de tracts sur une place publique. C'est une forme d'expression où chacun peut communiquer et publier son point de vue. Avec l'Internet, on est au cœur même de la liberté d'expression et celle-ci doit être entourée de la plus haute protection. Dans ces conditions, il est impossible d'adapter la régulation de l'audiovisuel à Internet.

Dans cet arrêt, la Cour a précisé qu'en matière de liberté d'expression sur Internet, aucun *effet réfrigérant* (« *chilling effect* ») n'est toléré. La première conséquence d'un tel effet, comme l'a soutenu la CJUE dans l'arrêt *Sabam Scarlet* de 2011[174], peut se résumer ainsi : une règle visant un contenu illicite de type A, risque de déborder et de bloquer certains contenus licites de type B. Dans ce cas, cela constitue une restriction excessive de la liberté d'expression. En d'autres termes, aucun effet de débordement n'est toléré.

L'autre aspect de l'effet réfrigérant est plus subtil. Pour le comprendre, il faut utiliser l'image de la « marmite ». Le marché des idées est une grande marmite bouillonnante dont la température doit rester élevée pour continuer d'offrir aux citoyens tous les ingrédients nécessaires à un débat libre. En conséquence, tout règlement de l'État qui tend à contraindre les moyens d'expression des citoyens entraîne une baisse de la température de la marmite en créant un effet réfrigérant sur le bon fonctionnement du marché des idées. L'effet réfrigérant peut se manifester à travers le comportement des intermédiaires techniques, qui vont, par peur des conséquences, s'autocensurer et réduire ainsi leur niveau d'activité, entraînant par là-même un appauvrissement du marché des idées. Les lois limitant la responsabilité des intermédiaires techniques visent à réduire ces effets d'autocensure.

2. Qu'en est-il en matière de territorialité ? Les États-Unis sont souvent critiqués pour l'effet extraterritorial de certaines lois (par exemple : « *antitrust, sanctions or discovery laws* »). Généralement, ces lois visent à réprimer des crimes ou des délits commis à l'intérieur des États-Unis ; mais leurs effets peuvent se sentir en dehors des États-Unis, comme le montre l'exemple récent des sanctions prises à l'encontre des banques de certains pays. En matière d'administration de la preuve devant les juridictions américaines (« *discovery* »[175]), les tribunaux américains commencent à tenir compte des principes européens de protection de données personnelles. En application du principe de *courtoisie internationale* (« *international comity* »), les tribunaux américains doivent tenir compte des lois et des intérêts de pays étrangers lorsqu'ils adoptent une décision ayant un effet extraterritorial. Ces lois étrangères ne s'imposent pas nécessairement aux tribunaux américains, mais ceux-ci doivent en tenir compte et, si possible, rendre une décision qui n'est pas en contradiction avec elles.

173 *U.S. Supreme Court*, 19 Mars 1997, *Reno vs American Civil Liberties Union*, n° 96-511.

174 CJUE, aff. C-70/10, 24 novembre 2011, *Scarlet Extended*.

175 La procédure de « *discovery* » est une procédure d'avant-procès conçue pour permettre la révélation d'informations entre demandeur(s) et défendeur(s) à travers des questions orales ou écrites, ou d'autres dispositifs (demande de production de documents, témoignages, etc.).

Dans ce contexte, *quid* de la territorialité en matière d'Internet ? Nous allons traiter cet aspect à travers un exemple connu. Tout le monde a entendu parler de l'affaire *Yahoo* où le tribunal de grande instance français enjoignit à cette société de retirer des objets nazis d'une vente en ligne[176]. C'était le premier cas de frottements de ce type. Comme le siège de *Yahoo* est aux États-Unis, la société a saisi la justice américaine pour plaider que la décision française était contraire à la liberté d'expression. Le tribunal de première instance américain a rejeté la demande de *Yahoo* pour des raisons de procédure, mais a validé l'idée selon laquelle la décision française était contraire à la Constitution américaine[177].

La décision de la Cour d'appel du neuvième district était plus réfléchie et nuancée[178] : les juges d'appel américains ont, en 2004, annulé le jugement rendu par la Cour de San José pour des questions procédurales puis, sur le fond, en 2006, ont refusé d'étendre la liberté d'expression américaine au territoire français en relevant que « *la France est un pays souverain* » et que *Yahoo* « *doit faire face à ses responsabilités en cas de violation des législations étrangères* ». Cette affaire fait ainsi apparaître le concept de respect des décisions étrangères dès lors qu'elles ne contreviennent pas fortement à des principes de lois de police américaines. Ainsi, si la règle étrangère est *répugnante* (en anglais, « *repugnant* ») par rapport aux principes américains, on ne peut pas l'exécuter. En revanche, s'il existe une certaine compatibilité on l'applique.

Cela nous conduit à la question du droit à l'oubli et à l'arrêt *Google Spain*. La première question est de savoir si un tel droit est compatible avec le droit des États-Unis. Pour cela, il faut se référer à la notion d'*effet réfrigérant*. Existe-t-il un risque de baisse de la température de la marmite où bouillonnent les idées ? La plupart des universitaires qui étudient la question pensent que le droit à l'oubli, tel qu'il est exprimé par la CJUE, serait contraire au premier amendement car il viserait des contenus qui sont parfaitement licites, même s'ils sont gênants pour la personne concernée (étant rappelé que le droit à l'oubli concerne des informations qui sont licites mais qui créent des effets négatifs pour la personne concernée).

Mais le débat n'est pas clos pour autant. Le droit à l'oubli n'est pas compatible avec le droit interne américain, mais pouvons-nous reconnaître une décision européenne qui imposerait à un moteur de recherche d'appliquer ce droit à l'oubli ? La réponse est dans l'affaire *Yahoo* : si les effets se cantonnaient à l'Europe, un tribunal américain pourrait reconnaître la décision. En revanche, si la décision prétendait limiter le droit à l'information d'internautes américains, ou prétendait limiter la liberté d'expression d'un éditeur situé aux États-Unis, la réponse serait clairement non.

On en revient à la question des barrières techniques et de l'étanchéité des prestataires de l'Internet. Chacun sait qu'il existe des *murs* qui permettent de filtrer des contenus pour certaines populations. Ces murs sont rapidement franchissables par les internautes. En revanche des murs vraiment infranchissables ça n'existe pas, sauf dans des pays totalitaires où tout le trafic Internet passe par une seule porte d'accès.

176 Ordonnance du TGI de Paris du 20 novembre 2000.

177 Cour fédérale de San José (Californie du nord), décision du 7 novembre 2001.

178 Cour d'appel du neuvième district de Californie, arrêts des 23 août 2004 et 12 janvier 2006, *Yahoo! Inc. vs la LICRA et l'UEJF*.

Bénédicte Fauvarque-Cosson
Professeur à l'université Panthéon-Assas,
présidente de la Société de législation comparée

Merci pour cet exposé qui permet de mieux comprendre la force de cette liberté d'expression et comment elle vient se heurter à certaines de nos préoccupations. Cette idée d'extraterritorialité croisée que vous avez évoquée a aiguisé ma curiosité et j'aimerais vous entendre plus longuement sur le sujet.

Édouard Geffray
Secrétaire général de la CNIL

L'idée autour de « *l'extraterritorialité croisée* » est de dire qu'il est impossible aujourd'hui de concevoir notre environnement juridique comme étant exclusivement territorial. On le voit bien lorsque l'on parle du droit au déréférencement : dans certains cas, la législation européenne peut avoir des effets qui dépassent ponctuellement le strict cadre géographique de ses frontières. De la même façon, les droits étrangers vont avoir des effets extraterritoriaux qui vont s'appliquer à des ressortissants français.

Je me méfie des chimères qui consistent à croire que l'on peut bâtir des murailles en matière de protection des données. C'est évidemment faux puisque les données circulent. La vraie question dans ce cas est de trouver des moyens pour être certain que les droits fondamentaux ne soient pas méconnus.

Je me permets d'apporter une petite précision concernant le droit au déréférencement. Maître Maxwell disait que le droit à l'oubli s'appliquait à des contenus *a priori* licites et prenait l'exemple des journaux. J'attire simplement votre attention sur le fait qu'aujourd'hui, si l'on prend les statistiques de *Google*, qui est le principal titulaire des demandes de déréférencement, seulement 3 à 4 % des demandes de déréférencement concernent des articles de presse. 96 % des demandes concernent des informations autres : des commentaires laissés sur des sites et impossibles à supprimer faute d'idenfiants, des photos, etc. La question de la liberté d'expression doit donc s'analyser à l'aune du fait que très peu de demandes portent sur des journaux, à l'aune de la portée réelle des déréférencements qui n'est, une fois de plus, que la dé-corrélation d'un nom et d'un résultat. C'est-à-dire que le contenu reste trouvable à partir de n'importe quelle autre requête que mon nom et mon prénom.

Alain Strowel
Professeur à l'université Saint-Louis de Bruxelles
et à l'université catholique de Louvain

Le droit au déréférencement s'impose clairement aux moteurs de recherche, mais je me pose la question concernant les sites d'information qui comportent un outil de recherche intégré au site, permettant de localiser des informations et donc de

consulter utilement les archives du site. Le droit au déréférencement s'applique-t-il en ce cas ? Rappelons que la CJUE a bien distingué les obligations qui concernent l'opérateur qui propose un service de référencement (par exemple, *google.fr*) de l'obligation qui repose sur l'éditeur (par exemple, *lesechos.fr*). Il y a déjà de la jurisprudence nationale qui semble considérer qu'une obligation similaire de déréférencement vaut pour l'éditeur, mais les choses ne sont pas claires et il faut tenir compte de la responsabilité spécifique de chaque acteur dans la chaîne d'acheminement de l'information. Nous gagnerions à éclaircir cette question.

En ce qui concerne la liberté d'expression, le point de départ en Europe est sans doute le même qu'aux États-Unis. On protège la liberté d'expression avant tout face aux ingérences de l'État, mais la Cour de Strasbourg a reconnu un effet horizontal à l'article 10 de la Convention européenne des droits de l'homme[179].

Le débat autour du « *droit à l'oubli* » est appréhendé autrement en Europe, notamment parce nous n'avons pas seulement l'article 10, mais aussi l'article 8 de la Convention EDH concernant la vie privée et familiale. En principe, il n'y a pas de prééminence de l'un par rapport à l'autre, mais l'arrêt *Google Spain* de la CJUE précise toutefois que les droits à la vie privée (articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne) « *prévalent, en principe (…) sur l'intérêt d(u) public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne* ». Aux États-Unis, la Constitution ne reconnaît pas de la même façon – et de manière aussi horizontale – la vie privée et familiale, même si l'on peut lui trouver des fondements constitutionnels comme le montre l'arrêt de la Cour Suprême *Riley c/ Californie*[180]. Le droit à la vie privée et familiale n'est pas aussi déployé que celui qui s'est construit en Europe sur le fondement de l'article 8 de la Convention EDH qui va bien au-delà de la protection de l'intimité de la vie privée.

Enfin, on distingue en Europe les faces active et passive de la liberté d'expression. La face active, à savoir le droit de manifester ses opinions, est très forte ; par contre, la face passive de la liberté d'expression, à savoir le droit d'accès à l'information, n'a pas la même force en cas de concurrence avec d'autres droits ou principes fondamentaux. Est-ce qu'une pondération modulée selon la face en cause fonctionne de la même façon aux États-Unis ? En tout cas, la façon dont les pondérations sont faites peut avoir une influence pour l'analyse du droit au déréférencement qui met en jeu le droit d'accès à l'information.

179 « *1. Toute personne a droit à la liberté d'expression. Ce droit 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. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations. 2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire* », Convention européenne des droits de l'homme (Convention EDH), art. 10, liberté d'expression.

180 U.S. Supreme Court, 25 juin 2014, *Riley v. California*, n° 13-132, 573 U.S.

Édouard Geffray

Secrétaire général de la CNIL

L'arrêt de la CJUE du 13 mai 2014 *Google Spain* ne crée pas un droit nouveau (le droit au déréférencement), mais se borne à reconnaître l'application du droit à l'effacement et du droit d'opposition aux moteurs de recherche.

Imaginons un site de presse avec des articles référencés par un moteur de recherche externe au site. Mes droits à l'égard de l'éditeur du site et à l'égard d'un moteur de recherche sont *a priori* les mêmes. Simplement, si je m'adresse au moteur de recherche, l'unique effet de ces droits ne peut être que le déréférencement, c'est-à-dire la sortie d'un résultat de la liste. Rappelons que ce droit est conditionné, dans tous les cas, à un motif légitime ou à l'aspect périmé ou erroné de la donnée à caractère personnel.

Si je m'adresse à l'éditeur du site, les deux procédures étant indépendantes et autonomes selon la CJUE, l'éditeur a une totale liberté d'action pour arriver au résultat : il peut choisir entre l'anonymisation de l'article, sa suppression ou sa désindexation (d'un moteur de recherche interne ou externe). Pour information, en règle générale, le site de presse désindexe l'article sur les moteurs de recherche externe ou l'anonymise. Il est très rare qu'il supprime l'article !

Winston Maxwell

Avocat associé à Hogan Lovells

Sur la question des phases active et passive de la liberté d'expression, il doit être noté que la jurisprudence américaine se concentre sur celui qui s'exprime en premier. La protection de celui qui reçoit l'information est certes reconnue, mais avec une intensité un peu moins forte que la liberté de s'exprimer.

Bénédicte Fauvarque-Cosson

Professeur à l'université Panthéon-Assas,
présidente de la Société de législation comparée

Nous avons parlé du droit à l'oubli. Il y a également le droit de ne pas communiquer les données personnelles dont on dispose; sur cette question Marc Mossé pourra nous éclairer.

Marc Mossé

Directeur des affaires juridiques et publiques,
membre du comité de direction de Microsoft France

C'est une agréable sensation que de traverser l'Atlantique pour, en atterrissant le jour d'après, continuer à parler du sujet que l'on évoquait la veille en partant. Pourtant, il s'agit d'un sentiment de continuité pas si étrange si l'on considère que le numérique aime à se jouer du temps et de l'espace et que précisément cette capacité liée à son architecture décentralisée, qu'accentue *l'informatique en nuage* (en anglais « *cloud computing* »), pose de nombreuses questions sur l'application

territoriale du droit. Le thème de notre table ronde et, plus largement, le sujet de l'étude annuelle 2014 du Conseil d'État sont, en réalité, des sujets véritablement transnationaux car ils traitent des questions à portée universelle.

Libertés individuelle et personnelle, ordre public et sécurité, rôle de la puissance publique et des acteurs privés, cyber sécurité, droit applicable et garanties pour le citoyen, place du juge et du régulateur, etc., constituent quelques-uns des ingrédients d'une réflexion plus large sur les conséquences d'une nouvelle révolution industrielle à l'œuvre qui transforme nos sociétés et interroge le rôle de l'État et la place du citoyen. Cela nous oblige à imaginer ce qu'est désormais la souveraineté à l'ère numérique. Il est, à cet égard, une tendance consistant à évoquer les termes de souveraineté numérique de façon restrictive. Ainsi de *l'informatique en nuage national* qui, mal conçue, peut être une manière d'enfermer les nouvelles technologies dans des frontières artificielles au risque de reconstituer des *lignes Maginot numériques* dont on mesure qu'elles ne sont pas forcément les plus opératoires pour garantir les droits de chacun. Cette tentation protectionniste ne résout ni la question de la souveraineté des États, ni celle de la protection des libertés du citoyen.

La demande de souveraineté est plus que légitime et il importe d'y apporter des réponses adéquates, en considérant que la complexité des situations en apparence nouvelles ne dispense pas de respecter les principes fondateurs de nos sociétés.

Il se trouve que nous sommes, chez *Microsoft*, actuellement confrontés à cette tension se nouant autour des libertés et des frontières, autour de la protection des données personnelles et de la sauvegarde de l'ordre public. De quoi s'agit-il ? Le gouvernement américain a saisi *Microsoft* pour accéder, *via* un mandat, aux données d'un usager de nos services dont les courriels sont stockés dans notre centre de traitement de données de Dublin. Nous avons opposé un refus à cette demande. Nous comprenons que cette atteinte au droit fondamental qu'est le respect de la vie privée ait pu sembler justifiée au juge américain. Mais peut-il donner à sa décision une application extraterritoriale, imposant sa perception américaine des libertés et des limites qu'il est possible de leur apporter à l'Irlande où sont stockées les données ?

Sans surprise, le juge de New-York a rejeté cet argument, tout comme le juge supérieur. Et *Microsoft* est aujourd'hui assigné devant la Cour d'appel du second circuit de New-York, avec un débat à la fois sur la question de l'application extraterritoriale de la loi américaine et sur la portée de la protection de la vie privée et des données personnelles.

Cette affaire m'inspire à cet instant deux réflexions. Tout d'abord, concernant l'argument que nous avons développé qui est de dire qu'en droit américain il n'est pas possible de donner à une loi une portée extraterritoriale si le Congrès ne l'a pas expressément prévu. Cela a été jugé par la Cour suprême dans une affaire *Morrison* contre une banque australienne[181]. Nous revendiquons donc cet argument en disant que l'*Electronic Communications Privacy Act*[182] ne prévoit aucunement cette portée

181 *U.S. Supreme Court*, 24 juin 2010, *Morrison v. National Australian Bank LTD*, n° 08-1191.
182 *Electronic Communications Privacy Act* de 1986 (ECPA), 18 U.S.C. § 2510-22.

extraterritoriale du texte. Nous nous revendiquons aussi de la logique de l'arrêt *Charming Betsey,* une vielle décision de 1804[183], qui est de dire que le Gouvernement des États-Unis ne peut pas concevoir et appliquer une loi de telle sorte qu'elle viole le droit international et les engagements internationaux des États-Unis.

Ce qui est intéressant dans notre démarche, c'est que nous partîmes seuls, « *mais par un prompt renfort nous nous vîmes trois mille en arrivant au port* »[184]. Dans cette affaire, en effet, plus de cinquante organisations nous ont rejoint en produisant des *Amici curiae*[185]. Ce qui mérite l'attention, c'est qu'au-delà des « *usual suspects* » représentant toutes les organisations de défense des libertés civiques et des droits fondamentaux, il y a aussi les organisations du secteur industriel qui mesurent que ce sujet peut devenir une ombre portée sur la confiance que l'on peut avoir sur les services numériques. Mais il y a également des professeurs de droit, le Gouvernement irlandais qui soutient qu'il y avait une autre manière de faire *via* le traité d'assistance mutuelle judiciaire et même M. Albrecht, rapporteur du Parlement européen pour le projet de règlement sur la protection des données personnelles.

Chacun, sous des angles différents, s'exprime sur cette affaire qui pose des questions universelles. Je dis cela car nous avons une tendance à opposer l'Europe et les États-Unis sur cette question des droits fondamentaux. Certes, il existe des différences culturelles et d'appréciation, mais j'ai la conviction que se révèlent de plus en plus des valeurs communes qui, pour certaines d'entre elles, pourraient constituer une sorte de patrimoine constitutionnel mondial en matière de libertés numériques.

Nous disposons déjà d'un patrimoine constitutionnel européen. Je pense que nous pourrions construire un patrimoine constitutionnel mondial autour de ces sujets. Il conviendrait évidemment d'en définir le périmètre exact, mais nul doute qu'il couvrirait le sujet structurant de la protection des données personnelles et de la façon dont nous pouvons être tracé par des organisations privées ou publiques.

La dimension universelle de ces questions est d'autant plus certaine que, contrairement à une petite musique facile, l'Europe n'est pas la seule à s'interroger sur la façon d'appréhender les droits et libertés fondamentaux à l'ère du numérique.

On en voudra pour preuve la décision, encore assez peu commentée en France, de 2014 de la Cour suprême *Riley c/ Californie*[186], rendue à l'unanimité sur le fondement du quatrième amendement de la Constitution des États-Unis[187]. Sans

183 *U.S. Supreme Court*, 1804, *Murray v. The Charming Betsey*, 6 U.S. 2 Cranch 64.

184 Pierre Corneille (1606-1684), *Le Cid*, acte IV, scène 3.

185 L'expression latine *amicus curiae* (pluriel : *amici curiae*, amis de la cour) est une « *notion de droit interne anglo-américain désignant la faculté attribuée à une personnalité ou à un organe non-partie à une procédure judiciaire de donner des informations de nature à éclairer le tribunal sur des questions de fait ou de droit* » (J. Salmon, *Dictionnaire de droit international public*, Bruxelles, Bruylant, AUF, 2001, pp. 62-63).

186 *U.S. Supreme Court*, 2014, *Riley v. California*, n° 13-132.

187 « *Le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir* », Constitution des États-Unis, 4e amendement.

entrer dans le détail, on notera qu'une partie de l'opinion exprimée par le *Chief Justice* Roberts est très intéressante. De quoi s'agissait-il ? De la saisie par un policier du contenu stocké sur le *smartphone* d'un délinquant arrêté en flagrant délit. La Cour va considérer que pour saisir ces données, il convenait d'obtenir un mandat judiciaire dès lors qu'il en allait de données personnelles et donc de vie privée. Le juge Roberts relève dans son opinion que si la question est posée à propos d'un téléphone mobile, en réalité, de plus en plus de données sont stockées ailleurs que dans les appareils eux-mêmes et notamment dans *l'informatique en nuage.* Il n'en tire pas de conséquences immédiates pour cette décision, mais il est intéressant que le *Chief Justice* fasse dans son raisonnement le prolongement vers l'informatique en nuage pour dire que, maintenant, c'est en appréhendant le champ immense du stockage dématérialisé à partir duquel il faudra de plus en plus réfléchir en la matière. Logique si l'on considère l'idée que les données se déplacent dans le monde entier et, à leur façon, méconnaissent les frontières physiques telles que nous les avons toujours conçues.

Désormais, une forme de logique ubiquitaire s'installe et, avec elle, l'idée que la protection des libertés dans le monde physique ne peut s'affranchir de leur garantie dans le monde digital. Le domicile immatériel, qui peut être ici et ailleurs, doit alors être protégé au même titre que le domicile physique considérant que nos traces numériques peuvent parfois en dire bien plus que ce que l'on peut trouver dans notre logement, y compris via l'utilisation de métadonnées[188].

J'ai le sentiment qu'aujourd'hui il est nécessaire d'engager une discussion entre l'Europe et les États-Unis pour mettre au point un instrument international qui concilie protection des données, liberté des personnes et souveraineté des États, en clarifiant notamment un certain nombre d'éléments sur la protection des données personnelles et sur la préservation de l'ordre public. Il est temps de le faire, car les acteurs comme *Microsoft* se retrouvent parfois dans des situations compliquées, écartelés entre des demandes qui peuvent être contradictoires.

Il faut donc que l'Europe et les États-Unis s'entendent pour créer des principes communs, qui pourraient d'ailleurs passer par une harmonisation des traités d'assistance judiciaire mutuelle, avec des formulaires et des procédures communes simplifiées, harmonisées et accélérées. Car il est possible d'aller vite comme cela a été le cas lors de la tragique affaire de l'attentat contre *Charlie Hebdo* où les données qui nous ont été demandées sur les comptes courriels de certaines personnes ont été livrées en quarante-cinq minutes aux autorités françaises dans le respect des procédures. Écarter les procédures judiciaires au motif qu'elles seraient trop coûteuses ou trop longues n'est donc pas un bon argument. Il faut au contraire les perfectionner et les simplifier.

188 Il est selon moi regrettable que le Conseil Constitutionnel dans sa décision du 24 juillet 2015 rendue sur la loi relative au renseignement n'ait pas saisi l'opportunité de dessiner les contours d'un droit constitutionnel adapté aux menaces pesant sur les libertés à l'ère numérique et n'ait pas, s'écartant ainsi du raisonnement de la CJUE sur le même sujet, tiré toutes les conséquences de l'impact des métadonnées sur la vie privée. Ce qui aurait pu être une grande décision témoigne plutôt d'une mauvaise compréhension de ces enjeux de la part du Conseil Constitutionnel.

Bénédicte Fauvarque-Cosson
Professeur à l'université Panthéon-Assas,
présidente de la Société de législation comparée

Cela pourrait-il se réaliser dans le cadre des négociations sur le TTIP[189] ? Il y a des débats sur ces questions en ce moment et certaines entreprises, notamment aux États-Unis, y seraient très favorables.

Marc Mossé
Directeur des affaires juridiques et publiques,
membre du comité de direction de Microsoft France

Je ne pense pas que le TTIP soit le bon instrument, car les questions qui sont par exemple posées dans l'affaire du mandat de New York renvoient notamment à des problématiques liées aux procédures et à la coopération judiciaires. Ce n'est sans doute pas le bon cadre pour traiter de telles questions.

Bénédicte Fauvarque-Cosson
Professeur à l'université Panthéon-Assas,
présidente de la Société de législation comparée

Nous allons poursuivre ce débat et revenir sur la notion d'extraterritorialité avec Alain Strowel.

Alain Strowel
Professeur à l'université Saint-Louis de Bruxelles
et à l'université catholique de Louvain

J'ai découvert l'étude annuelle 2014 du Conseil d'État il y a quelques semaines. C'est un travail précieux, notamment par les propositions ambitieuses que l'on y trouve. N'étant pas aussi audacieux, je serai plus réservé sur les propositions qui consistent à vouloir mettre en évidence un *ordre public européen* ou à parler de *loi de police*. Si l'on débat de ces questions au niveau européen, on pourrait rencontrer assez rapidement des divergences de principe sur ces valeurs, comme en témoigne, par exemple, l'affaire *John Huston*[190].

En l'espèce, le film *Asphalt Jungle* (en français, *Quand la ville dort*) de John Huston avait été colorisé, en vue de sa diffusion à la télévision, sans l'accord du réalisateur et alors même que le film avait été intentionnellement tourné en noir et blanc, à une époque où la pellicule couleur existait. Les ayants droit de Huston ont attaqué devant les tribunaux français la chaîne française de télévision qui envisageait de diffuser la version colorisée – qui avait été licitement réalisée et diffusée ailleurs. Si le droit français était applicable, il y avait atteinte à l'intégrité

189 Partenariat transatlantique de commerce et d'investissement (PTCI), en anglais « *Transatlantic Trade and Investment Partnership (TTIP)* ».
190 Cour de cassation, 1e ch. civile, 28 mai 1991, bull. civ. I, n° 172.

du droit moral du réalisateur. Mais tous les facteurs de rattachement désignaient le droit américain comme le droit applicable. La Cour de cassation a jugé que les règles relatives au droit moral faisaient partie des règles de police, ce qui a eu pour effet d'évacuer la question du rattachement et d'appliquer le droit français de manière assez *unilatérale*. Je doute que beaucoup d'autres pays européens partagent le point de vue qui fasse du droit moral une règle aussi fondamentale que, par exemple, l'interdiction de la bigamie. J'en conclus qu'il faut être prudent dans notre approche des problèmes, tant les règles de droit sont différentes d'un pays à l'autre, et multiplier les lois de police n'est pas une solution satisfaisante dans le concert européen.

Mon exposé comportera deux parties. La première traitera du *droit des États dans l'univers transnational en ligne* ; je distinguerai à cette occasion les différents sens de la notion de territorialité et je reviendrai sur l'enseignement tiré de l'application du droit d'auteur. Dans la deuxième partie, je parlerai de *l'effet global du droit dans le domaine du numérique* où il faut certes parler du droit des États, mais ne pas oublier que le droit n'est pas que le droit des États. Il y a d'autres normes qu'il faut aussi solliciter pour réguler l'Internet.

1. Sur la territorialité du droit étatique, les choses sont complexes.

On peut repartir des conclusions récentes d'un avocat général à la CJUE, dans une affaire qui opposait le Royaume-Uni au Parlement européen et au Conseil et qui concernait le contrôle prudentiel des établissements de crédit[191]. Le Royaume-Uni, qui, depuis, s'est désisté de l'instance, contestait l'applicabilité de ces règles pour un comportement survenu hors Union européenne dans un groupe de sociétés. L'avocat général rappelle qu'il n'y a pas de principe de droit international empêchant un État d'étendre au-delà de son territoire la portée d'une législation. Il se fonde sur les grands arrêts du droit international de la Cour permanente de justice internationale (CPJI)[192], notamment sur la célèbre affaire du *Lotus*[193]. Du reste, les cas d'applicabilité extraterritoriale du droit se sont multipliés au cours des années[194].

Ensuite, l'avocat général distingue deux notions, à travers les termes anglais « *juridiction to prescribe* », la compétence pour prescrire des règles, et « *juridiction to enforce* », le pouvoir de mettre en œuvre la puissance publique dans le territoire d'un autre État.

Je pense qu'il faut faire cette distinction, comme le montrent les affaires *Google Spain* et celle, pendante devant le juge de New-York, dans laquelle *Microsoft* conteste une demande de perquisition des autorités américaines relative à

191 Conclusions de l'Avocat Général N. Jääskinen, *in* CJUE, aff. C-507/13, présentées le 20 novembre 2014, points 36 et suiv.

192 La CPJI, créée en 1922 suite à la Première Guerre mondiale, a été mise en place par le pacte de la Société des Nations (art. 14 du pacte de la SDN). Elle est remplacée en 1946, après la Seconde Guerre mondiale, par la Cour internationale de justice (CIJ), un organe de l'ONU.

193 Cour permanente de justice internationale (CPJI), affaire dite du « *Lotus* » (France c. Turquie) du 7 septembre 1927.

194 V. Fr. Rigaux, *Le concept de territorialité : un fantasme en quête de réalité*, in *Liber Amicorum Mohammed Bedjaoui*, La Haye, Kluwer Law International, 1999, pp. 211-222.

l'information stockée sur ses serveurs localisés en Irlande. Dans l'affaire *Google Spain*, ce qui est en cause c'est la territorialité au sens de la compétence d'imposer des règles, mais dans le cadre d'un traitement de données qui a des effets dans l'Union européenne. Dans ce cas-là, je pense qu'il n'y a pas d'application extraterritoriale du droit protégeant les données personnelles.

Reste toutefois la question encore discutée de l'étendue de l'obligation de déréférencement : si elle s'applique clairement aux versions européennes .fr, .be, etc. du moteur de recherche, *Google* refuse de l'étendre au site google.com, comme l'exige la CNIL. Je constate que les recherches faites à partir de l'Europe sur google.com sont systématiquement redirigées vers un site national (par exemple, les requêtes faites à partir d'un terminal en France sur google.com aboutissent à une page sur google.fr), et le problème est donc largement théorique. Seul l'usage de *serveurs proxy* ou d'autres manipulations permettent à quelqu'un basé en Europe de faire une recherche sur google.com. Si les résultats sont accompagnés de publicités ciblées vers le pays de celui qui introduit la requête, je pense que l'obligation de déréférencement s'applique à google.com. L'étendue géographique du droit de déréférencement est en réalité largement fonction de l'usage d'instruments de géolocalisation des requêtes et des réponses (et des publicités associées).

Je suis plus prudent en ce qui concerne les contraintes de la territorialité pour la mise en œuvre du droit lorsque c'est l'autre type de compétence qui est en cause (« *jurisdiction to enforce* »), comme dans l'affaire *Microsoft* pendante devant le juge de New-York.

Quelques réflexions relatives à l'applicabilité du droit national peuvent ensuite être faites en creusant l'analogie entre les droits de la personnalité et les droits d'auteur. Il y a des parallèles, car nous avons des droits fondamentaux qui protègent la vie privée et le droit d'auteur. Le droit d'auteur est consacré à l'article 17 paragraphe 2 de la Charte des droits fondamentaux de l'Union européenne[195] ; dans certains pays, il est protégé à la fois par des dispositions constitutionnelles sur la propriété et sur le droit à l'auto-déploiement de la personnalité. En Allemagne, le droit d'auteur repose sur ces deux fondements. Ce qui veut dire que l'opposition entre *propriété* et *autodétermination* n'est pas pertinente; il vaut donc mieux penser en terme de *continuum* avec comme caractéristique commune de ces droits la maîtrise sur l'information, à l'instar d'un auteur sur son œuvre ou d'un individu sur ses données personnelles.

Dès lors, la jurisprudence concernant le droit d'auteur sur Internet peut être une référence pour penser certains problèmes d'applicabilité du droit à la protection de la vie privée sur les réseaux. Récemment, la CJUE dans ses arrêts *Pinckney* de 2013 et *Pez Hedjuk* de 2015[196] a mis en évidence le critère « *d'accessibilité du site Internet* » pour définir la juridiction compétente. Ce critère diffère de celui de la *focalisation* (le site vise-t-il le public français ?) appliqué habituellement pour déterminer le droit applicable à une action délictuelle pour atteinte au droit d'auteur. Lorsque le

195 « *La propriété intellectuelle est protégée* », Charte des droits fondamentaux de l'Union européenne, art. 17, § 2.

196 CJUE, aff. C-170/12, 3 octobre 2013, *Peter Pinckney c. KDG Mediatech AG* ; CJUE, aff. C-441/13, 22 janvier 2015, *Pez Hedjuk c. EnergieAgentur*.

défendeur est hors de l'Union européenne, on a de la jurisprudence en matière de droit d'auteur, notamment de la Cour d'appel de Paris ou de Bruxelles, qui a rendu le droit français ou le droit belge applicable pour toute une série d'opérations qui sont réalisées en ligne par *Google*, éventuellement en dehors des frontières nationales, dès lors que des actes d'exploitation visent ces pays.

Un usage combiné des critères d'*accessibilité* pour la compétence juridictionnelle et de *focalisation* pour le droit applicable serait utile pour une résolution effective des conflits touchant à la vie privée, par un tribunal proche des personnes affectées. Cela pourrait être discuté sur la base du nouveau règlement européen. Toute la question demeure toutefois de savoir si le modèle de la juridiction étatique est adéquat pour trancher les mini-litiges en ligne. On pourrait plaider pour un système alternatif de règlement de ces litiges afin d'éviter que *Google* ou d'autres moteurs de recherche demeurent les *seuls juges de l'oubli*, ce qui est le cas actuellement (sous la réserve des plaintes introduites devant les autorités en matière de vie privée par ceux dont les demandes de déréférencement n'ont pas été acceptées par les moteurs de recherche).

2. Pour ce qui concerne l'effet global du droit, je souhaiterais tout d'abord évoquer un premier point : le dialogue des juges[197]. La présence du droit étranger dans le raisonnement du juge interne est quelque chose de très précieux qu'il faut préserver et développer. La Cour EDH emprunte, par exemple, des arguments à la Cour suprême des États-Unis, elle l'a fait notamment en matière de liberté d'expression avec l'arrêt *Barthold*[198] sur l'applicabilité de l'article 10 de la Convention EDH au discours commercial. Dans d'autres affaires, la Cour de Strasbourg se réfère à la Cour Suprême du Canada. C'est donc tout à fait positif. Inversement, la Cour suprême des États-Unis le fait également mais de façon plus timide. La décision précitée *Riley c/ Californie* de 2014, par exemple, ne fait pas référence à la jurisprudence de la Cour européenne des droits de l'homme ; on n'a pas ce dialogue des juges qui ouvrirait la voie à la convergence des points de vues sur le sujet de la vie privée, déjà traité en profondeur par la Cour de Strasbourg. Je reste donc quelque peu sceptique quant à cette *solution*.

Le deuxième point concerne *l'effet bruxellois* (en anglais, « *The Brussels Effect* »). Il ne s'agit pas de l'imposition impérialiste d'une réglementation européenne adoptée à Bruxelles, mais du fait que le marché européen étant incontournable pour les opérateurs privés, ceux-ci ne peuvent pas l'ignorer et doivent donc aussi se conformer *de facto* aux prescriptions de Bruxelles. Cet effet bruxellois est donc une forme de globalisation unilatérale de la régulation[199]. On n'impose pas le droit, mais comme tous les opérateurs privés souhaitent vendre et s'adresser à des consommateurs européens sur le marché européen, ils doivent s'y conformer.

Aux États-Unis, patrie du numérique, il semble qu'il y ait un effet californien du même type. On oppose d'ailleurs souvent *l'effet Delaware* (en anglais, « *Delaware*

197 J. Allard, *Le dialogue des juges à la Cour européenne des droits de l'homme et à la Cour suprême des États-Unis. Constats et perspectives philosophiques*, in J. Allard et al., *Juger les droits de l'homme : l'Europe et les États-Unis face à face*, Bruylant, 2008.

198 CEDH, requête n° 8734/79, 25 mars 1985, *Barthold c. Allemagne*.

199 A. Bradford, *The Brussels Effect*, *Northwestern Law Review*, 2012, vol. 107/1, pp. 1-67.

Effect »), sorte de concurrence à la baisse pour attirer les entreprises, à *l'effet californien* à la hausse lié au fait que la Californie a des régulations plus strictes, notamment en matière d'environnement. Une entreprise d'une certaine taille opérant aux États-Unis ne peut pas ignorer le marché californien ; elle doit donc respecter les normes adoptées en Californie. L'effet bruxellois, c'est la même chose au niveau européen, voire mondial. Je pense que cela fonctionne déjà assez bien pour le droit de la concurrence, et cela commence à fonctionner pour le droit de la vie privée. Ma conviction est qu'il faut plutôt compter sur cet effet-là pour résoudre les problèmes d'extraterritorialité. Cet *effet bruxellois* les dissout en réalité.

Troisième point : outre le droit des États, il faut également tenir compte d'autres normes. Réfléchissons un instant à la fiscalité des acteurs du numérique. Que peut-on faire pour assurer le paiement d'une taxe juste alors que la cessibilité des droits de propriété intellectuelle permet aux grands acteurs du numérique de loger les actifs immatériels dans des paradis fiscaux ? Il y a évidemment le droit de la concurrence, le droit dur, celui des aides d'État. La Commission européenne enquête dans plusieurs affaires mettant en cause notamment *Apple* et *Amazon*.

On peut également utiliser le *droit souple* défini par l'OCDE, qui élabore des règles notamment en matière fiscale pour éviter que les sociétés ne se délestent de leurs bénéfices pour éviter de payer l'impôt sur les sociétés. Il faut en tenir compte. Mais le problème, c'est que pour certains droits fondamentaux, nous n'avons pas d'organismes internationaux qui élaborent du droit souple.

Une autre norme, dont les effets ne sont pas à sous-estimer, est la *réputation*. La réputation d'une entreprise a des effets très importants sur son déploiement. On peut considérer par exemple que c'est le risque en termes de réputation qui a poussé *Google* à prendre en 2014 la décision de quitter les paradis fiscaux où elle faisait de l'optimisation fiscale agressive. La volonté des opérateurs économiques d'afficher un comportement éthique pour entretenir une image positive auprès des clients est un facteur dont les actions publiques doivent tenir compte. En tant que juriste, on a tendance à ignorer ce facteur, il ne faut pas le négliger. Cela signifie aussi que la responsabilité sociétale des entreprises (notamment en matière fiscale et de vie privée) est à étoffer et rappeler, parce qu'elle peut orienter les conduites des entreprises.

Il y a donc le droit des États, comme le règlement général en matière de vie privée en discussion au Parlement et au Conseil de l'Union européenne. Mais il ne faut pas pour autant oublier le droit souple et d'autres formes de normativité qui peuvent permettre de résoudre certains problèmes d'extraterritorialité.

Bénédicte Fauvarque-Cosson
Professeur à l'université Panthéon-Assas,
présidente de la Société de législation comparée

Vous ouvrez là une perspective intéressante. Quelle est l'efficacité du droit souple quand il s'agit de protéger les droits fondamentaux ? Ce processus prend-il beaucoup de temps ? Est-il suffisamment contraignant pour les entreprises ?

Alain Strowel
Professeur à l'université Saint-Louis de Bruxelles
et à l'université catholique de Louvain

Je pense que le droit souple est plus agile et plus rapide que le droit étatique, et donc les acteurs intéressés à la création de ces normes nouvelles, telles les ONG ou certaines enceintes internationales, pourraient jouer un rôle de précurseurs. Je suis d'accord pour dire que cela ne suffit pas, mais on ne peut pas négliger l'effet de ces normes de droit souple car, pour réguler les réseaux mondiaux, le droit des États ne suffit pas.

Bénédicte Fauvarque-Cosson
Professeur à l'université Panthéon-Assas,
présidente de la Société de législation comparée

Cela dit, on peut penser au *pacte mondial* des Nations unies (en anglais, « *Global Compact* ») qui est une initiative internationale d'engagement volontaire en matière de responsabilité sociétale des entreprises.

Marc Mossé
Directeur des affaires juridiques et publiques,
membre du comité de direction de Microsoft France

Cette approche du droit souple est très intéressante, c'était d'ailleurs le thème de l'étude annuelle 2013 du Conseil d'État[200], car elle permet d'imaginer des réponses agiles à des problématiques mouvantes.

Je suggère ici de travailler à partir d'un triptyque dynamique : régulation, corégulation et autorégulation.

Pour le premier volet, il faut redire que l'on ne peut pas faire l'économie de la régulation posée à travers des principes de droit forts ; une sorte de droit source qui irrigue par ses principes et qui est mis en œuvre sous des formes diverses adaptées à la vitesse des technologies. Le projet de règlement de l'Union européenne sur les données personnelles en est un bon exemple. Ce pourrait même être demain un instrument international fixant des règles en matière de transfert de données ou sur les conditions d'accès aux données par les autorités étatiques. Des principes simples sont ici sans doute plus utiles qu'une réglementation excessivement complexe.

Le second volet est celui de la corégulation. Il s'agit là de faire vivre les principes par un dialogue constant entre les régulateurs et toutes les parties prenantes. Par exemple, si l'on s'intéresse à l'informatique en nuage (en anglais, « *cloud computing* »), nous avons inclus des clauses contractuelles types, prévues par la décision de la Commission 2010/87/CE du 5 février 2010, dites clauses « *de*

200 Droit souple (en anglais, « *soft law* »). V. aussi Conseil d'État, étude annuelle 2013, *Le droit souple*, ed. La documentation Française.

responsable de traitement à sous-traitant », à travers un dialogue avec le Groupe de l'article 29. De la même façon, les règles internes d'entreprises en matière de données personnelles (en anglais, « *binding corporate rules* ») sont un bon exemple de corégulation. Ce second volet permet donc de faire vivre la régulation de façon efficace et en l'adaptant.

Le troisième volet est celui de l'autorégulation. Il ne doit pas s'agir, à mon sens, d'un substitut à toute régulation étatique mais, au contraire, de la possibilité pour certains acteurs d'aller plus loin, s'ils le veulent, que ce que la réglementation impose. Cette autorégulation s'ajoute alors à la régulation étatique et à la corégulation. C'est l'idée que l'innovation responsable peut faciliter la création de nouveaux produits et services tout en intégrant dans les processus industriels les préoccupations des citoyens et des consommateurs. C'est l'exemple de la « *privacy by design* » (en français, protection de la vie privée intégrée dans un système dès la phase de sa conception) dans laquelle nous sommes engagés et qui permet l'« *empowerment* » de l'utilisateur c'est-à-dire un plus grand contrôle de chacun sur ses données tout en pouvant accéder à des nouveaux services, etc. C'est en jouant sur ces différentes touches que l'on pourra, dans l'avenir, appréhender les questions et les défis posés par le numérique et rendre à la souveraineté sa dimension essentielle : non pas tant celle de surveiller des frontières ou des citoyens à l'intérieur des frontières, mais bien celle de protéger les droits fondamentaux de chacun.

Échanges avec les participants

Question *- Je voudrais revenir sur la distinction entre phase active et phase passive de la liberté d'expression. La liberté d'expression repose sur un émetteur et un récepteur, il me semble donc que les deux phases devraient être protégées de manière égale.*

Winston Maxwell

Aux États-Unis, la liberté de recevoir l'information est reconnue. Je crois que les spécialistes de droit constitutionnel font une distinction entre les deux phases, mais c'est très théorique. La Cour suprême dans sa vision a indiqué qu'Internet est comme une personne qui rentre dans une grande bibliothèque. On est vraiment dans une démarche du citoyen qui cherche l'information, il y a donc également une protection du récepteur.

Question *- J'ai une question pour M. Maxwell, qui reprend le chiffre de M. Geffray selon lequel le déréférencement concerne assez peu d'articles de presse, mais surtout du contenu mis en ligne par les utilisateurs. Cela nous renvoie à la question de savoir si le droit à l'oubli aurait un effet réfrigérant. À l'inverse, on pourrait penser que le droit à l'oubli existe justement pour empêcher un tel effet : à chaque fois que nous nous retrouvons face à une audience mixte sur Internet, nous pouvons avoir des cas d'autocensures liées au fait que des commentaires conçus pour une certaine audience se retrouvent repris dans un autre contexte : on parle de « context collapse ». Cela peut entraîner un effet de gel de la conversation, avec l'anticipation de cette collision des contextes.*

Winston Maxwell

La littérature sur le droit à l'oubli aux États-Unis est vraiment balbutiante. Les articles d'universitaires que j'ai lus n'en effleurent encore que la surface. Nous ne sommes pas au stade où nous pouvons apprécier toute la complexité de cette question, et il faudra attendre plusieurs années pour en arriver à une réflexion plus poussée.

Question *- Dans les différences de valeur entre l'Europe et les États-Unis, j'ai l'impression qu'il existe une différence sensible sur le passé de délinquant d'une personne. Il semblerait qu'en Europe le droit à l'oubli pousse à faire table rase de ce passé, alors qu'aux États-Unis on considère qu'il peut être dans l'intérêt du public d'être au courant du passé de délinquant de quelqu'un.*

Winston Maxwell

Il est toujours difficile de généraliser, mais c'est assez juste globalement, même s'il existe des exceptions concernant par exemple les délinquants mineurs.

Alain Strowel

La consécration par la CJUE du droit au déréférencement a surpris : ce droit trouve son fondement dans une directive existante en matière de données personnelles alors même que l'on discutait de son introduction dans la proposition de règlement général sur la protection des données... À lire l'arrêt de la CJUE, ce droit est aussi – et surtout ? – fondé sur une pondération entre les libertés fondamentales. De ce point de vue, le droit au déréférencement n'est pas quelque chose de nouveau, car le droit à l'oubli existe en France, en Allemagne et en Belgique, depuis assez longtemps, en cas de divulgation d'informations d'ordre judiciaire (du type par exemple de celles divulguées dans l'affaire Google Spain).

***Question** - La protection des droits fondamentaux est souvent représentée comme un frein à l'activité économique. Ne peut-on pas voir cela comme un avantage ? Je pensais au projet allemand d'informatique en nuage où les entreprises, du fait qu'elles appliquent le droit de l'Union, en font un argument de vente.*

Question - Quid *de la pratique qui se développe, notamment en Grande-Bretagne, où lorsqu'un État veut faire fermer un site, plutôt que de s'adresser à l'hébergeur, il s'adresse de manière informelle et sans contrôle du juge à l'opérateur du nom de domaine et lui demande de rayer ce nom de la liste des sites ? Est-ce une bonne pratique et faut-il réintroduire le rôle du juge dans ce processus ?*

***Question** - A-t-on vraiment besoin d'un nouveau cadre juridique pour réguler Internet ? Ne peut-on pas utiliser les outils administratifs et juridiques existants ?*

***Question** - Enfin, pourriez-vous repréciser la notion de patrimoine constitutionnel mondial ? Quels en seraient le contenu et la portée ?*

Marc Mossé

Pour revenir sur la première question, la règle de droit n'est pas nécessairement un obstacle à l'innovation, au contraire. En revanche, je suis assez réservé sur la solution d'une informatique en nuage strictement localisée entre les frontières – on a le même débat en France qu'en Allemagne – dès lors qu'existe un cadre européen et des normes internationales. Je suis assez réservé sur cette idée, car elle aboutirait à recentraliser tout en la fragmentant une architecture qui, par nature, est décentralisée. En outre, et surtout, je ne pense pas que sur le fond cela induise une meilleure garantie des droits pour les utilisateurs. Même avec des serveurs localisés près de chez vous, si l'opérateur ne respecte pas certains standards de sécurité, la proximité des serveurs ne donne pas plus de garantie que s'ils étaient dans un autre État. Ces standards peuvent provenir du droit dur ou du droit souple, telles les normes ISO qui se développent de plus en plus, comme par exemple la norme ISO 27018, spécifique à l'informatique en nuage qui est une norme naissante, à l'élaboration de laquelle la CNIL a d'ailleurs participé et pour laquelle nous avons été les premiers certifiés.

En résumé, je ne suis pas certain que la localisation des serveurs au sein d'un État soit la solution unique à ces questions légitimes de souveraineté. Il y a aussi une raison économique à ce doute : le principe économique derrière l'idée de l'informatique en nuage est la mutualisation, seule capable de générer des économies d'échelle. Si chaque État décide de développer son « nuage souverain », on créera peut être des champions nationaux de l'informatique en nuage, mais pas des champions internationaux, et les économies d'échelle risquent de ne pas être au rendez-vous.

À l'inverse, encore une fois, cela ne veut pas dire qu'il ne faut pas mettre en place des normes très exigeantes, notamment au niveau européen. D'où l'importance du règlement européen actuellement en discussion[201] dont l'une des qualités est l'harmonisation du droit au sein des États de l'Union ; qualité qu'il convient de préserver alors qu'on aborde la phase du trilogue.

Alain Strowel

Je voudrais revenir sur la question de la création d'une nouvelle catégorie de prestataires intermédiaires qui se verraient imposés une responsabilité particulière. Je suis réservé sur cette question. La présentation des différents rôles que Google joue et des différentes fonctionnalités que l'on peut trouver sur YouTube, notamment une faculté de stockage personnel, montrent la difficulté de qualifier le rôle de ces opérations et de ces entreprises. Ce sont des questions que l'on doit analyser au cas par cas, en fonction du rôle des intermédiaires. Je pense que si l'on garde la séparation entre éditeur et hébergeur, on peut y arriver. Par contre, il pourrait être utile de mieux savoir à partir de quand un hébergeur joue un rôle actif et non purement automatique qui a pour effet de lui retirer le bénéfice de l'exonération de responsabilité. C'est une question qui pourrait être traitée à travers un instrument de droit souple, comme par exemple une norme ISO sur les intermédiaires hébergeurs. De la même façon que l'on a une norme ISO sur la responsabilité sociétale des entreprises, on pourrait en avoir une sur la responsabilité en ligne, quitte à ce que ces directives souples soient réintégrées un jour à la directive 2000/31 sur le commerce électronique[202]. Pour l'instant, le débat semble clos, on ne veut pas ajouter une quatrième exonération de responsabilité en Europe ; tandis qu'aux États-Unis il y en a quatre. Sans doute est-il préférable de tester, notamment à travers le droit souple, les avantages et les inconvénients d'une meilleure qualification des rôles des intermédiaires en ligne.

Marc Mossé

Avant de répondre à la question sur le patrimoine constitutionnel mondial, je souhaiterais vous conseiller la visiter du site digitalconstitution.com où l'on a rassemblé l'ensemble des mémoires échangés dans « l'affaire du juge de New York » que j'ai évoquée précédemment.

201 Il s'agit d'une réforme globale des règles adoptées par l'Union européenne en 1995 en matière de protection des données personnelles proposées, dont le groupe de travail se nomme « article 29 ».

202 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (dite « *directive sur le commerce électronique* »).

Je reste conscient de la modestie et de l'insuffisance de ma réponse face à la question de ce que pourrait être un patrimoine constitutionnel mondial en la matière, mais je voudrais redire qu'un dialogue Europe - États-Unis est nécessaire. S'il aboutissait à quelque chose de concret, ce serait un moteur puissant pour d'autres régions du monde, car le couple Europe - États-Unis pèse dans l'économie mondiale. Et si ce changement reflétait la demande des internautes désireux d'obtenir une meilleure protection de leurs droits fondamentaux, aucun acteur économique ne pourrait s'extraire de telles exigences.

Nous sommes à un moment clé de l'histoire humaine où les questions du numérique font ressortir les différences culturelles entre pays et testent les capacités d'adaptation de toutes nos organisations, États compris. Ces changements révèlent des enjeux civilisationnels profonds et interrogent la capacité des femmes et des hommes politiques à ne pas se laisser dominer par la technique ; et l'étude annuelle 2014 du Conseil d'État est sur ce point remarquable, car elle va loin dans la réflexion, notamment sur la question des algorithmes. Je pense que si l'on arrive à enclencher cette discussion au niveau international, et qu'une force citoyenne s'empare du sujet, on pourra bâtir les fondations d'une vision audacieuse des droits de l'homme à l'ère numérique. Il serait dommage de ne pas saisir cette opportunité historique pour que la transformation de nos sociétés se réalise sur une base de confiance.





Séance de Clôture – conclusion à deux voix

Maryvonne de Saint Pulgent,
présidente de la section du rapport et des études du Conseil d'État

Diplômée de Sciences Po Paris et ancienne élève de l'ENA, Maryvonne de Saint Pulgent est la présidente de la section du rapport et des études du Conseil d'État depuis le 30 avril 2014. Elle a commencé sa carrière en 1976 comme conseillère au tribunal administratif de Paris. Elle a intégré en 1980 la Cour des Comptes en tant que rapporteur, puis le Conseil d'État en 1986 comme maître des requêtes. Commissaire du gouvernement près l'assemblée du contentieux et les autres formations de jugement du Conseil d'État de 1987 à 1993, elle est devenue présidente de la 8e sous-section du contentieux en 2001. En 2003, elle a intégré la section de l'intérieur. Maryvonne de Saint Pulgent a été directrice du Patrimoine au ministère de la culture et de la francophonie et présidente de la caisse nationale des monuments historiques et des sites, de 1993 à 1997. Depuis 2007, elle préside le comité d'histoire du ministère de la culture. Présidente de la Maison de l'histoire de France de janvier à septembre 2012, Maryvonne de Saint Pulgent est également présidente du conseil d'administration du Théâtre national de l'Opéra Comique et du conseil d'administration de l'Institut géographique national.

Andreas Paulus,
juge à la Cour constitutionnelle fédérale d'Allemagne

Depuis 2006, Andreas L. Paulus est professeur de droit public et de droit international à l'université de Göttingen et, depuis 2010, juge à la Cour Constitutionnelle fédérale d'Allemagne. Rapporteur à la première chambre, qui traite des droits fondamentaux, il est chargé, entre autres, des domaines du droit d'auteur, de la liberté d'expression artistique, et du droit fiscal. Il a obtenu en 2006 le titre de privat-docent (en allemand « *Privatdozent* » pour maître de conférences) et en 2000 le titre de docteur en droit à l'université de Münich. En 2014, il a enseigné les relations entre divers systèmes de droit à l'université Panthéon-Assas à Paris II et à l'académie de droit constitutionnel à Tunis. M. Paulus a été conseil de l'Allemagne dans deux affaires à la Cour internationale de justice. Ses publications traitent notamment de la théorie du droit public international, du droit des Nations Unies, du droit pénal international et du droit constitutionnel. En outre, M. Paulus est coéditeur du commentaire principal anglais de la Charte des Nations Unies (Oxford UP, 2012).

Maryvonne de Saint Pulgent
Présidente de la section du rapport et des études du Conseil d'État

Le Conseil d'État a souhaité donner une forte dimension européenne à ce colloque, en témoigne la présence de deux magistrats allemands, dont Andreas Paulus qui est à mes côtés, de deux universitaires belges, d'un avocat américain au barreau de New-York qui travaille aussi à Paris et que nous considérons comme un Européen même si ce n'est pas son origine, et de deux responsables de filiales françaises de grandes entreprises américaines.

Cette dimension européenne et internationale s'imposait. D'abord parce que le numérique a d'emblée une dimension internationale. Les données ignorent les frontières et les traversent facilement. Cependant, Internet met en permanence en relation et parfois en conflit le droit des États, des internautes et des sites qu'ils consultent. Cela a été l'un des fils rouges de ce colloque.

La deuxième raison, c'est que nombre de sujets évoqués ici relèvent d'une action de l'Union européenne et des normes européennes, même si les États membres conservent une marge de manœuvre non négligeable.

C'est avec de tels dialogues entre européens, mais aussi avec des représentants d'autres espaces juridiques, qu'une conception européenne des droits fondamentaux à l'ère du numérique peut émerger.

Cet exercice est à la fois nécessaire et difficile, d'autant que nous ne partons pas des mêmes traditions juridiques. En raison de nos histoires nationales, le droit à la vie privée n'a pas toujours la même sensibilité ni le même contenu pour tous. Je parle ici des divergences de vue à l'intérieur de l'Europe, sachant que nous avons aussi évoqué les différences de sensibilité entre l'Europe et les États-Unis d'Amérique.

Les enjeux de sécurité nationale peuvent également justifier, comme l'admet la jurisprudence de la Cour européenne des droits de l'homme, certaines restrictions aux droits fondamentaux. Ces enjeux se posent dans des termes différents selon les pays de l'Union européenne.

Dans ce contexte, cet exercice de réflexion supranationale est devenu particulièrement nécessaire. Sur Internet, les rapports de droit peuvent sans doute passer par un dialogue des juges, mais j'ai toujours eu tendance à penser que ce sont également des rapports de force. Nous sommes incontestablement plus forts à cinq cents millions d'internautes européens qu'à soixante-cinq millions d'internautes français. C'est *l'effet bruxellois* évoqué par M. Strowel.

L'Europe, par ailleurs, fait face à un défi économique. Elle est aujourd'hui distancée dans l'économie numérique par les Américains et bientôt par les Chinois. Cela menace sa prospérité.

La réponse à ce défi ne peut pas se passer d'une réflexion sur son cadre juridique parce que l'économie numérique met en jeu les droits fondamentaux que sont la protection des données personnelles, la liberté d'expression, la liberté

d'entreprendre et, comme l'a fait observer Édouard Geffray, d'autres libertés – même si c'est de façon plus marginale – comme la liberté d'aller et venir ou le droit de vote.

Définir une conception européenne des droits fondamentaux à l'ère du numérique n'exclut nullement le rapprochement avec d'autres espaces juridiques, et pas seulement l'espace américain, au sens des États-Unis d'Amérique. Les Européens sont moins isolés qu'ils ne le pensent dans la défense de leurs valeurs. Nous avons cité dans l'étude annuelle 2014 du Conseil d'État la « *Marco Civil da Internet* » brésilienne, Constitution de l'Internet au Brésil adoptée en avril 2014[203], qui consacre nombre de principes qui nous sont familiers. Dans le même esprit, la Corée du Sud, l'une des nations les plus dynamiques dans le numérique, s'est dotée en 2011 d'une loi très protectrice de la vie privée. Sur la neutralité de l'Internet, la convergence entre l'Europe et les États-Unis est à l'œuvre ; mais, pour dialoguer avec les autres et dans de bonnes conditions, pour construire ensemble des traités ou des accords de droit souple, il faut d'abord savoir quelles conceptions nous, nations européennes, avons en commun et pouvons partager.

C'est pour cette raison que les contributions de ce colloque, qui participent de cette construction européenne des droits fondamentaux, ont porté sur les trois sujets essentiels que sont : la protection des données personnelles, la régulation des plateformes et la territorialité du droit.

Sur la protection des données personnelles, des appels à renouveler notre conception du sujet ont donné un vif intérêt à la première table ronde. Nous avons entendu un appel à envisager les données personnelles comme une propriété de l'individu ou comme un travail de celui-ci. Nous n'avons pas toujours partagé ce point de vue, qui contribue pourtant de façon fertile à la réflexion collective puisque nous cherchons encore la bonne manière d'appréhender cette réalité nouvelle. Je crois cependant que la voie que nous proposons, et qui se dessine en Europe, comme le montrent les travaux sur le projet de règlement européen et comme l'ont illustré plusieurs interventions, est celle d'une réaffirmation des principes construits sur notre continent depuis quatre décennies : principe de détermination des finalités de l'utilisation des données, principe de proportionnalité, rôle exercé par les autorités indépendantes de contrôle et de régulation.

Cette réaffirmation des principes doit aller de pair avec une profonde rénovation de leurs instruments. L'arrêt *Google Spain* de la CJUE du 13 mai 2014 dont il a été largement question l'illustre bien. C'est à partir des droits d'opposition et de rectification, qui existent depuis longtemps, que la Cour de justice a forgé ce système nouveau du droit au déréférencement des moteurs de recherche. Ce droit continue de faire débat, mais c'est en tout cas une régulation effective de la société numérique actuelle qui a été bâtie par la Cour de justice à partir de principes connus de notre ordre juridique. C'est donc dans le même esprit que nous avons proposé de rallier notre droit interne français à la conception allemande de l'autodétermination informationnelle.

203 *Marco Civil da Internet* loi n° 12.965 du 23 avril 2014.

J'ai également entendu un appel à l'application du droit patrimonial seulement dans son volet droit moral. Cependant, nous n'avons pas l'habitude de séparer le droit moral du droit patrimonial, et cela nous obligerait à une novation assez forte du droit d'auteur. Nous avons d'ailleurs évoqué cette piste lors de la préparation de l'étude pour, finalement, penser que le droit à l'autodétermination informationnelle aboutissait au même résultat que l'institution d'un droit moral. Il nous a paru en tous cas très difficile d'admettre un droit économique des données personnelles, un droit susceptible d'être monnayé qui nous parait avoir beaucoup trop d'inconvénients, que l'on pense à l'utilisation des données personnelles par les services publics ou à la cession d'un droit patrimonial hors partie droit moral.

La question des plateformes a également été fortement discutée, même si le sujet est beaucoup plus technique et économique que la question des données personnelles qui, elle, touche véritablement aux droits de la personne. Cette seconde table ronde a montré à quel point les débats sur la définition même du phénomène des plateformes et les formes appropriées de sa régulation restaient denses et nourris. Néanmoins, il ne faut pas oublier que l'étude ne propose pas de faire entrer les plateformes (au sens des *Google*, *Apple*, *Facebook* et *Amazon*) dans une nouvelle catégorie juridique qui s'appliquerait à toutes leurs activités. Elle cherche à appréhender un nouveau type d'activité qui n'est ni celle d'hébergeur, ni celle d'éditeur, et qui n'est pas traitée juridiquement dans notre droit européen.

Bien entendu, et pour répondre à des observations qui ont été faites par les intervenants, c'est uniquement l'activité de plateforme au sens d'activité de référencement, de classement et d'indexation qui serait appréhendée par le régime juridique que propose l'étude annuelle 2014 du Conseil d'État.

En tout cas, personne n'a contesté, et Nicolas Colin en a bien montré l'importance, l'existence de cette réalité nouvelle, de ces acteurs nouveaux qui jouent un rôle incontournable dans l'économie numérique et dans la prescription des contenus les plus consultés par les internautes. Le fait qu'ils exercent par ailleurs des activités identifiées dans les textes ne les rend pas moins importants, et n'interdit pas d'appréhender par le droit cette activité non traitée juridiquement.

Puis, j'ai entendu Christian Paul affirmer que le vrai sujet est celui des algorithmes. En tout cas nous sommes d'accord sur un point avec Christian Paul : ce sujet-là, bien qu'omniprésent dans notre vie, n'est pas traité dans notre droit, et cette omission devra être corrigée.

Sur la territorialité du droit, sujet qui concerne bien d'autres domaines qu'Internet et préoccupe beaucoup le Conseil d'État, nous avons vu à quel point Internet fait entrer le droit international privé dans la vie quotidienne. La troisième table ronde a montré toutes les difficultés que cela présente pour les institutions, les entreprises, les citoyens et les juges. Un tel phénomène se révèle pour les citoyens et pour les États une menace par le fait que les règles de droit national, protectrices des citoyens, peuvent être écartées par un renvoi contractuel à une loi étrangère. Il ne faut cependant pas y répondre par une multiplication des lois extraterritoriales, avec les conflits de lois qui en résulteraient. De ce point de vue, l'affirmation par le règlement européen de son extraterritorialité serait, certes, importante, mais ne résoudrait pas tous les problèmes.

C'est pourquoi, nous avons réfléchi à une distinction entre les droits fondamentaux pour lesquels les États européens ne pourraient, en aucun cas, renoncer à assurer la protection de leurs citoyens, sauf garantie d'une protection équivalente, et les autres règles de droit pour lesquelles le jeu habituel des conflits de loi et de résolution de ces conflits pourrait être accepté. Et ceci pour répondre aux inquiétudes légitimes sur le caractère excessif des lois de police. Bien sûr, la conception que nous proposons est une conception vraiment limitée au noyau dur des règles de protection et, dans ce sens, nous avons bien entendu la mise en garde de M. Strowel sur le problème qu'il y aurait à qualifier de loi de police n'importe quel niveau de droit, ce qui ne serait pas une réponse pertinente.

L'étude 2014 du Conseil d'État n'écarte pas pour autant d'autres pistes. Elle n'écarte certainement pas le droit souple et fait beaucoup de préconisations dans ce domaine, avec la conviction qu'il faut savoir l'utiliser. Elle n'écarte pas non plus la voie de la négociation internationale d'un traité, sachant que dans une négociation l'important est ce que l'on fait en amont pour se préparer au rapport de forces qui préside à toute discussion. C'est peut-être le moment idéal pour conclure un traité euro-américain ; mais nous avons beaucoup de projets de traités euro-américains sur la table et ils ne sont pas tous rassurants du point de vue de la protection des droits des États et des citoyens européens. Nous sommes tout à fait d'accord pour emprunter cette voie, mais il faut le faire avec des armes qui nous permettent de bien négocier ces tournants.

Enfin, je voudrais rappeler que faire des propositions sur le numérique c'est toujours prendre des risques dont, surtout, celui de l'obsolescence rapide : les innovations se succèdent à une telle vitesse que nous avons nous-mêmes, dans le court moment des neuf mois de travail de l'étude annuelle, vu se transformer le sujet sous nos yeux, notamment à travers les deux grands arrêt de la Cour de justice de l'Union européenne des mois d'avril et de mai 2014 dont il a été beaucoup question : *Digital Rights Ireland* et *Google Spain*.

Je remercie les intervenants à ce colloque, dont certains nous ont accompagnés pendant l'étude annuelle 2014 à travers ce que nous avons appelé le groupe de contact, et les nombreux participants venus pour échanger sur ces enjeux de la transformation numérique dont tout le monde mesure l'importance pour notre avenir.

Andreas Paulus
Juge à la Cour constitutionnelle fédérale d'Allemagne

Je me réjouis d'avoir l'honneur et le plaisir de conclure ce colloque qui a été extrêmement riche sur le plan des idées. L'étude annuelle 2014 du Conseil d'État apparaît comme particulièrement utile, car elle participe au dialogue des juges et des juridictions, au dialogue avec la société européenne et aussi au dialogue international. Cette contribution importante pourrait permettre d'aboutir au développement d'une pratique commune internationale même si, au préalable, il reste beaucoup d'éléments à préciser et à mettre en œuvre.

Au début de ce colloque, M. le vice-président Sauvé a évoqué le défi auquel nous sommes confrontés : faire face à un développement technologique et social extrêmement rapide avec un droit qui, structurellement, est incapable de réagir rapidement face à ces évolutions. Or, si le droit ne réagit pas, le danger existe d'aller vers quelque chose que nous ne voulons pas : un Internet qui ne respecte pas les droits fondamentaux qui sont au cœur du développement juridique européen depuis un millénaire au moins. Je me réjouis donc que le droit à l'autodétermination informationnelle, qui est une innovation de la Cour constitutionnelle fédérale d'Allemagne, figure d'une façon prééminente dans cette étude.

Les intervenants de la première table ronde ont débattu pour savoir si ce droit à l'autodétermination informationnelle provenait des caractéristiques intrinsèques des données. Je ne pense pas que cela soit aussi simple. Car, au-delà des aspects qui relèvent de la propriété intellectuelle ou du droit d'auteur, dans leur dimension financière et économique, il existe également un aspect moral très important du droit à l'autodétermination. Dans ce contexte, c'est au législateur qu'il revient de trouver un équilibre entre les divers droits individuels concernés, notamment le droit de propriété (avec ses conséquences en matière sociale) d'une part, et les droits de la société d'autre part, et de s'assurer que cet équilibre soit compatible avec le droit international public et privé en vigueur.

Si l'on analyse les deux arrêts de la Cour de justice de l'Union européenne de 2014, *Digital Rights Ireland* et *Google Spain*, deux aspects ressortent qui, en droit allemand, sont distincts. D'un coté, ce sont les droits contre l'État et la collecte de données qu'il réalise. De l'autre, c'est le devoir de l'État, à travers la législation et la jurisprudence, de veiller à ce qu'un équilibre existe entre les droits des particuliers (citoyens ou entreprises). Cette juxtaposition est fondamentale parce que la collecte, l'utilisation et le transfert des données doivent être légalement autorisés, quand bien même les entités privées peuvent (en théorie) négocier entre-elles de façon autonome leurs échanges de données sans, ou avant, que l'État n'y intervienne.

Pendant la première table ronde, nous avons vu que les internautes sont considérés comme responsables de leurs actes, même s'ils ne lisent pas la description des droits qui leurs sont imposés par les plateformes ou les sociétés informatiques. Certes, la réalité est biaisée puisque les utilisateurs de ces outils numériques n'ont pas vraiment le choix face au contrat qu'on leur propose car, en cas de refus, ils sont dans l'impossibilité d'utiliser les services sollicités. Il ne s'agit donc pas vraiment d'une négociation équitable. D'où le besoin de mettre en place une législation adaptée à ce nouveau paradigme. C'est là un manque qui relève non pas de la responsabilité de la Cour de justice de l'Union européenne, mais du législateur européen. En effet, dans la réalité il n'y a pas vraiment de mécanisme qui rende effectif ce droit à l'oubli en dehors du bon vouloir d'une société privée, principalement *Google*, décidant seule pour savoir quelles informations figureront ou non dans les résultats de la requête des internautes. Ce n'est donc pas une solution satisfaisante dès lors qu'il peut y avoir une présomption d'atteinte à des droits fondamentaux.

Dans les autres tables rondes, nous avons pu constater qu'il n'existe pas seulement un droit informationnel, mais aussi un droit à l'information, qui figure d'ailleurs dans la loi fondamentale pour la République fédérale d'Allemagne (article 5, al. 1er). Mais il y a encore d'autres droits qui sont également impliqués. Tout cela nécessite des nouveaux mécanismes institutionnalisés pour que les droits du public à l'information soient sauvegardés aussi, et non pas seulement le soi-disant droit à l'oubli de la partie requérante. Pour cela, nous avons besoin du législateur européen, car la Cour de justice de l'Union européenne ne peut pas créer des obligations qui n'existent pas encore dans la loi ! Il y a donc un besoin de développer la législation en la matière, et aussi de créer des nouvelles institutions pour pouvoir mieux répondre à ces défis.

Ce qui apparaît nécessaire également, comme le préconise le Conseil d'État, c'est de mettre en place une régulation pour la collecte des données qui puisse être jugée acceptable par la Cour de justice de l'Union européenne. Si l'on ne peut pas prévoir à l'avance quel en sera le résultat, une chose est sûre cependant, et le président de chambre von Danwitz l'a bien précisé, la durée de vie de certaines données collectées ne peut pas excéder deux ans[204]. D'autre part, on notera la nécessité de mieux utiliser les droits nationaux existants avant toute autre décision de la part des institutions européennes y compris de la Cour de justice. Enfin, on doit tenir compte du *fait de la vie privée* (en anglais, « *fact of privacy* ») dont a parlé M. Casilli et aussi de l'ambivalence des données évoquée par Mme Rahal-Löfskog qui peuvent constituer en même temps des sources de bénéfices et de risques pour le citoyen. La prise en compte de ces deux aspects est importante pour le respect des droits fondamentaux à l'ère du numérique.

Nous avons évoqué dans la deuxième table ronde le sujet de la régulation des plateformes. On pourrait ainsi en conclure que le droit à l'autodétermination informationnelle est une contribution allemande, tandis que le besoin de la régulation des plateformes pourrait être une contribution française à cette régulation future du numérique en Europe, voire dans le monde ; sans que l'on puisse, pour ce dernier aspect, se retrancher derrière l'argument qui consisterait à dire que, comme cela n'existe pas encore dans les règlements ou les directives européennes, on ne peut rien faire. Ce besoin est réel car les plateformes font plus que de l'hébergement.

C'est pourquoi nous avons besoin de nouvelles règles pour parvenir à une régulation équilibrée entre tous les acteurs de l'Internet. Nous avons également parlé durant ce colloque des différents types de confiances. Pourquoi faisons-nous confiance, par exemple, à *Facebook* s'il s'arroge le droit de cartographier notre navigation sur Internet ? Parce que nous avons besoin de ces services ! Cela nous amène donc à constater qu'il faut mettre en place une régulation du comportement de ces entreprises. Quant à l'énigme de cette confiance accordée aveuglément par les internautes, elle réside surtout dans le besoin d'utilisation de ces services qui semblent d'une qualité bien supérieure à tout ce que proposent les entreprises françaises et européennes du secteur.

204 V. l'arrêt de la CJUE *Digital Rights Ireland Ltd*, aff. C-293/12 du 8 avril 2014, paragr. 16, art. 6 au sujet de la directive 2006/24/CE.

Enfin dans la troisième table ronde, nous avons abordé un thème qui m'est cher : la territorialité du droit. Étant aussi professeur de droit international, je constate que l'évolution rapide des nouvelles technologies de l'information et de la communication est vraiment un défi pour le droit international. Depuis deux ans, des négociations ont lieu avec les États-Unis d'Amérique au sein du Conseil des droits de l'homme des Nations Unies. Pour les droits relatifs à l'Internet, il existe même une résolution de l'Assemblée générale, ainsi que des propositions communes allemandes et brésiliennes. Il serait intéressant d'unifier ces approches avec les tentatives internationales. Quant aux « *droits dont les personnes jouissent hors ligne, ils doivent également être protégés en ligne, y compris le droit à la vie privée* »[205].

Dans ce contexte, il est important de réaliser des études comme celle de 2014 du Conseil d'État sur le numérique et les droits fondamentaux. Si nous n'avons pas de principes internationaux, nous devons au moins essayer de développer un patrimoine constitutionnel mondial au niveau des sociétés. Pour ce faire, il est utile d'utiliser aussi les moyens du droit international privé évoqués dans la troisième table ronde.

Comme toujours dans le droit international privé, nous avons noté que les approches sont différentes, notamment entre les deux rives de l'océan Atlantique. Serons-nous capables de trouver un équilibre acceptable entre l'Europe et les États-Unis d'Amérique ? Cela n'est pas certain. C'est la raison pour laquelle nous avons besoin d'un dialogue des juges constant et, aussi, comme l'a évoqué M. le vice-président Sauvé, du contrôle d'une juridiction (suprême) qui défende les droits fondamentaux des citoyens européens désormais enrichis d'une nouvelle composante qui est le droit du numérique. Ce colloque constitue l'exemple d'un tel dialogue, car il permet par sa richesse d'approfondir la réflexion et d'offrir des pistes pour l'action. Par conséquent, il faut continuer à faire fructifier cet esprit, non pas de conflit de lois, mais de dialogue entre les lois.

205 V. la résolution adoptée par l'Assemblée générale sur la base du rapport de la Troisième commission (A/68/456/Add. 2) du 18 décembre 2013, « Le droit à la vie privée à l'ère numérique », doc. A/RES/167/68 du 21 janvier 2014, p. 2, paragr. 3.

(*source* : Conseil d'État, section du rapport et des études).

Algorithme : Programmes informatiques permettant, par exemple, de parcourir de grandes quantités de pages pour y détecter les bons indices et renvoyer les réponses correspondant aux questions de l'utilisateur. Les algorithmes ont plusieurs utilités : routage d'informations, cryptographie, ou encore planification. L'entreprise *Google* utilise dans ses algorithmes plus de deux cents signaux ou indices permettant de trouver les réponses adéquates aux recherches des utilisateurs. On y trouve entre autres les termes figurants sur les pages Internet et les actualisations de contenus.

Autodétermination informationnelle : Le concept d'autodétermination informationnelle a été consacré par la Cour constitutionnelle fédérale allemande en 1983 qui a établi, sur le fondement des articles 1er (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale allemande, que « *la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* ». C*f. infra* Annexe 3 pour un historique plus précis de cette notion.

Big data (mégadonnées) : Phénomène recouvrant à la fois l'expansion du volume de données et l'expansion de la capacité à les utiliser. Le « *big data* » est ainsi la possibilité d'exploiter des données nombreuses, hétérogènes (textes, images, données de connexion, données de localisation, etc.) et non structurées sous forme de bases de données. La commission générale de terminologie et de néologie retient également le terme de *données massives* (J.O. du 22 août 2014).

Cloud computing (l'informatique en nuage) : Système d'accès par le réseau à des ressources informatiques mutualisées, mobilisables et configurables à la demande. Les ressources informatiques sont fournies par des entreprises spécialisées et peuvent être des logiciels, des équipements informatiques, des plateformes de développement d'applications ou encore des capacités de stockage de données. On distingue généralement le « *cloud privé* » (les ressources du prestataire sont dédiées à l'utilisateur) du « *cloud public* » (les ressources sont mutualisées, une même ressource peut servir aux besoins de plusieurs utilisateurs).

Cookie : Fichier de petite taille sous forme de texte, enregistré sur le disque dur d'un ordinateur. La présence d'un tel fichier résulte de la demande du serveur gérant le site Web sur lequel se trouve l'internaute. Le « *cookie* » vise essentiellement à mémoriser, sur un site Internet donné, les habitudes et préférences exprimées par l'internaute lors d'une ou de plusieurs visites, de manière à lui proposer à nouveau des préférences exprimées lors d'une visite ultérieure.

Crowdfunding : Technique de financement, principalement des jeunes pousses, consistant à rechercher auprès de milliers de personnes les ressources nécessaires à la phase d'amorçage des projets de ces jeunes entreprises à croissance rapide.

Crowdsourcing (externalisation ouverte, production participative) : Utilisation par les éditeurs de sites des compétences d'un grand nombre d'internautes pour créer des contenus ou même participer à la conception du site. Le « *crowdsourcing* » passe généralement par un appel ciblé ou ouvert selon la spécificité des tâches en question.

Cryptologie : Du grec « *kryptos* » qui signifie caché et de « *logos* » qui signifie science, la cryptologie renvoie à la science du secret. Il s'agit de dissimuler les informations contenues dans un message. On peut identifier trois objectifs principaux de la cryptologie : assurer la confidentialité, garantir l'authenticité et conserver l'intégrité des informations.

Data brokers : Terme désignant des individus ou des sociétés qui exploitent et commercialisent des données personnelles.

Déréférencement : Toute personne a, en principe, le droit d'obtenir d'un moteur de recherche qu'il n'affiche pas certaines informations le concernant, même si ces informations ne lui sont pas préjudiciables. Le *droit au déréférencement* a été consacré dans l'ordre juridique de l'Union européenne par l'arrêt de la Cour de justice de l'Union européenne du 13 mai 2014 *Google Spain c/ AEPD*.

Données personnelles : Elles ont été définies par l'article 4 de la loi du 6 janvier 1978 qui a retenu une approche large de la notion. Ainsi constituent des données personnelles « *les informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou une personne morale* ».

Éditeur : Personne ou société publiant des pages sur Internet. L'éditeur de site Internet sélectionne les contenus, les assemble, les hiérarchise et les met en forme au moyen d'un support de communication en ligne. Les contenus mis en ligne par l'éditeur engagent sa responsabilité civile et pénale. À titre d'exemple, la société *eBay* a reçu la qualification d'éditeur par la Cour de justice de l'Union européenne ainsi que par la Cour de cassation dans la mesure où elle exerce un rôle actif lui permettant d'avoir une connaissance ou un contrôle des données stockées.

FabLabs (contraction de l'anglais « fabrication laboratory »* ou *laboratoire de fabrication) : Concept né au Massachusetts Institute of Technology dans les années 1990 désignant un lieu ouvert au public dans lequel, grâce à la mise à disposition d'outils de fabrication standard ou numérique, il est possible de concevoir divers types d'objets. Ces objets peuvent à l'avenir être commercialisés par leur concepteur.

Fournisseur d'accès à Internet (FAI) : Organisme (généralement une entreprise) offrant une connexion au réseau informatique Internet. Le terme anglais désignant un FAI est « *Internet service provider* » (ISP).

Hébergeur : Acteur destiné à mettre à disposition des internautes des sites Internet conçus et gérés par des tiers. Les internautes peuvent ainsi avoir accès aux contenus déposés dans leurs comptes par les webmestres. Contrairement aux éditeurs, les hébergeurs ont une responsabilité limitée.

ICANN (« Internet Corporation for Assigned Names and Numbers »* ou *Société pour l'attribution des noms de domaine et des numéros sur Internet) : Société de droit californien à but non lucratif qui assure la régulation d'Internet. L'ICANN est notamment chargée de gérer les ressources numériques d'Internet, comme l'adressage IP ou encore les noms de domaine de premier niveau.

Intelligence artificielle : Quête de techniques à même de rendre les systèmes informatiques comparables à des êtres humains en termes de capacités intellectuelles.

Interface de programmation d'applications (« application programming interface »* ou *« API ») : Elle a pour fonction la facilitation du travail d'un programmeur en mettant à sa disposition les outils premiers nécessaires. L'API est donc une interface sur laquelle se fondera un travail plus poussé de programmation.

Internet des objets : Conception d'Internet fondée sur des connexions entre objets fonctionnant de manière autonome. Les connexions entre robots forment une part grandissante du trafic Internet. L'Internet des objets est rendu possible par la convergence de trois évolutions technologiques : la capacité de donner à un objet un identifiant unique, reconnaissable à distance par d'autres objets, et ainsi de lui attribuer une adresse Internet ; l'effondrement du prix et de la taille des capteurs pouvant transmettre en temps réel une multitude de données ; et le développement de réseaux de communication sans contact en mesure de transmettre ces données.

IP tracking : Pratique commerciale interdite consistant à garder en mémoire l'adresse IP de l'internaute désireux d'acheter un bien en augmentant le prix du bien en question à chacune de ses visites afin d'accélérer la décision d'achat.

Keylogger : Catégorie de logiciels espions présentant la particularité d'enregistrer l'ensemble des saisies sur un clavier d'ordinateur, y compris des informations sensibles comme des mots de passe et des identifiants bancaires qui auraient été saisis pour une commande en ligne. Un « *keylogger* » peut être contenu dans un périphérique branché sur un ordinateur.

Logiciel espion (« spyware ») : Logiciel malveillant qui pénètre dans un ordinateur afin de collecter et transférer diverses informations de l'ordinateur, le plus souvent à l'insu de son utilisateur.

Marché pertinent (*ou *de référence) : Lieu de rencontre de l'offre et de la demande de produits ou de services dits « *substituables* » ou considérés comme tels par les utilisateurs ou les acheteurs.

Métadonnées : Données techniques de connexion comportant des informations sur d'autres données. Les métadonnées regroupent des données très variées telles que les adresses IP, les numéros de téléphone de l'appelant et de l'appelé, leur géolocalisation, la date et la durée de la communication.

Massive online open course (MOOC) : Formation Libre et Ouverte à Tous (FLOT), le « *MOOC* » est un type de formation permettant à chacun de suivre un enseignement à distance et de se faire évaluer, un système de *badges* et non de diplômes au sens classique sanctionnant généralement la participation avec succès au cours.

Moteur de recherche : Outil permettant de recenser les pages Internet. Contrairement aux annuaires, le moteur de recherche fait l'inventaire de pages Internet que des robots répertorient en parcourant les différents liens des pages présentes sur la toile. Chaque moteur possède un algorithme spécifique définissant son fonctionnement.

Navigateur Internet (« web browser ») : Logiciel informatique permettant l'accès à Internet.

Neutralité du Net : Concept formulé pour la première fois par le juriste américain Tim Wu, la neutralité du Net implique que tous les opérateurs doivent traiter de manière égale tous les flux de données, quels que soient leurs contenus. La neutralité repose sur le principe du *meilleur effort*. Il existe toutefois différentes conceptions de la neutralité du Net en fonction de la priorité laissée pour des raisons techniques aux services spécialisés (ou services gérés).

Numérique : Par opposition à l'analogique, le numérique qualifie une représentation de l'information par un nombre fini de valeurs discrètes.

Octet : Unité de mesure de huit bits permettant de coder une information. Le terme octet (symbole « o ») est le plus souvent employé pour caractériser les capacités de mémoire des appareils électroniques, des multiples de l'octet, comme le kilooctet (Ko) ou le mégaoctet (Mo) existant également. L'octet par seconde mesure la vitesse de transmission d'informations.

Open data (données ouvertes) : Le terme désigne une orientation de politique publique ayant pour objet de rendre accessibles à tous *via* Internet des données publiques non nominatives collectées par les organismes publics.

Opt-in / opt-out : « L'*opt-in* » consiste à obtenir l'autorisation préalable de l'internaute avant de pouvoir lui adresser un message ou encore pour collecter des données le concernant. « L'*opt-out* » consiste à enregistrer l'autorisation par défaut de l'internaute.

Over the top : Se dit d'un diffuseur utilisant l'infrastructure de l'opérateur afin de fournir son service. À titre d'exemple, *Facebook* ou encore *Netflix* sont des acteurs dits « *over the top* » en ce qu'ils utilisent le réseau Internet afin de fournir leur service.

Paquet télécoms : Ensemble de directives européennes régulant le secteur des télécommunications. En 2007, la Commission européenne a rendu public un projet de réforme de ces directives.

Passenger Name Record (PNR) data (données du dossier passager) : Informations collectées par les compagnies américaines et les agences de voyage dans le cadre des services de réservation. Les données collectées sont ensuite échangées entre les différentes entreprises intervenant de la réservation à la réalisation des prestations demandées. Le dossier passager peut notamment contenir les renseignements sur l'agence de voyage par laquelle le client a effectué sa réservation, ou encore l'itinéraire du déplacement qui peut comporter plusieurs étapes.

Phishing (hameçonnage) : Technique utilisée par des escrocs pour collecter des données personnelles sur Internet. Les fraudeurs peuvent par exemple prétendre être un organisme bancaire pour obtenir un mot de passe ou un numéro de carte bancaire à des fins de détournement de fonds.

Plateforme : Structure de travail grâce à laquelle on peut écrire, développer mais aussi utiliser des logiciels. Au sens de l'étude 2014 du Conseil d'État, les plateformes sont entendues dans un sens plus large. Ainsi les prestataires intermédiaires fournissant un service de classement de contenus, les moteurs de recherche, les réseaux sociaux ou encore les magasins d'applications feraient partie de cette définition. En revanche la catégorie de plateforme n'inclurait pas les acteurs ayant une responsabilité directe dans la mise en ligne des contenus, tels certains sites de musique en ligne ou de vidéo à la demande.

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 discrimination et sans garantie de résultat.

Privacy by design : Protection de la vie privée intégrée dans un système dès la phase de sa conception. Le « *privacy by design* » est donc pensé comme un moyen de prévenir dans la structure même d'un produit les atteintes à la vie privée.

Quantification de soi* ou *automesure (« quantified self ») : Mouvement marqué par la volonté de donner à chacun les moyens de mesurer, d'analyser mais également de partager ses données personnelles. Un *ordiphone* ou *terminal de poche* (« *smartphone* ») peut devenir un outil privilégié du « *quantified self* » en permettant à l'utilisateur de mesurer, par exemple, le nombre de pas effectués chaque jour ou encore de mesurer le pouls afin de prévenir d'éventuelles maladies cardio-vasculaires.

Reconnaissance faciale : Technique qui consiste à reconnaître une personne en analysant sa photographie en un temps très court. Cette technique recouvre trois étapes principales : une caméra prend la photographie du visage, le logiciel qui reçoit la photographie la numérise, puis il opère le traitement souhaité.

Réseaux sociaux : Ensemble des systèmes permettant une interaction numérique avec des groupes de personnes. On distingue généralement trois grandes catégories de réseaux sociaux : le réseau social de type relationnel (*Facebook* par exemple), le réseau social de type professionnel (*Viadéo* ou *Linkedin* entre autres), et le réseau social de type informationnel tel que *Twitter*.

Safe harbor (sphère de sécurité) : Ensemble de principes de protection des données personnelles négocié entre la Commission européenne et les autorités américaines en 2001. Les principes en question sont issus des règles posées par la directive 95/46 du 24 octobre 1995, en ce qui concerne notamment l'information des personnes, le consentement explicite pour les données sensibles, la sécurité des données. Une entreprise américaine peut adhérer volontairement au « *Safe harbor* » et certifier qu'elle se conforme à la législation européenne en ce domaine pour transférer des données personnelles de l'Union européenne vers les États-Unis.

Services de médias audiovisuels à la demande (SMAD) : Services de communication au public par voie électronique permettant le visionnage de programmes au moment choisi par l'utilisateur et sur sa demande, à partir d'un catalogue de programmes dont la sélection et l'organisation sont contrôlées par l'éditeur de ce service.

Services gérés : Pour l'ARCEP, on désigne par services gérés « *tout service d'accès à des contenus/services/applications par voie électronique proposé par un opérateur bénéficiant, pour certains paramètres, de caractéristiques améliorées par rapport à celles de l' « accès à Internet ». Il s'agit notamment de garanties supérieures (« premium ») fournies par l'opérateur en termes de bande passante garantie, de perte de paquets, de gigue, de temps de latence, ou encore de sécurité du réseau accrue* ». Entrent par exemple dans ces services gérés les offres dites « *triple play* » incluant la téléphonie fixe, la télévision sur Internet et l'accès à l'Internet haut débit.

Spam : Pour la CNIL, le « *spamming* » ou « *spam* » désigne l'envoi massif et éventuellement répété de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière. Le plus souvent, ces messages n'ont pas d'adresse valide d'expédition ou de « *reply to* », et l'adresse de désinscription est inexistante ou invalide.

Streaming (diffusion en flux) : Mode de transmission de données audio ou vidéo. Dans ce système, l'internaute dispose du fichier dès qu'il le sollicite, grâce au flux continu. Il n'y a donc pas besoin de téléchargement pour pouvoir lire le fichier en question.

Téléchargement de pair à pair (« peer to peer » ou P2P) : Technologie d'échange de fichiers entre internautes : deux ordinateurs reliés à Internet sont ainsi en mesure de communiquer l'un avec l'autre sans que le passage par un serveur central soit nécessaire.

Téléchargement direct : Le téléchargement direct désigne, par opposition au téléchargement en pair à pair, la mise à disposition de fichiers directement téléchargeables sur un site Internet.

World Wide Web : Plus souvent désigné sous le terme de *Web*, ou encore la Toile, le *World Wide Web* est un système hypermédia public permettant d'avoir accès aux ressources du réseau Internet. L'usage d'un navigateur de recherche permet d'y consulter les pages des différents sites.

3G : Génération de normes de téléphonie mobile. La 3G, grâce à des débits plus rapides que la précédente génération, permet des usages plus avancés tels que la visiophonie et le visionnage de vidéos en ligne.

4G : Norme de téléphonie mobile succédant à la 3G et permettant d'accéder au « très haut débit mobile » allant jusqu'à 100 ou 150 Mbits/seconde. La 4G permet des usages tels que le téléchargement, le visionnage et le partage rapides de photos et de vidéos.

Annexes





Annexe 1 : Résumé et propositions de l'étude du Conseil d'État, ***Le numérique et les droits fondamentaux***

(source : Conseil d'État, étude annuelle 2014, *Le numérique et les droits fondamentaux*, Paris, La documentation Française, 2014).

1. Résumé de l'étude

Mettre le numérique au service des droits individuels et de l'intérêt général

Aujourd'hui, les droits reconnus aux individus se limitent, pour l'essentiel, à leur permettre de rester à l'écart du traitement de leurs données (choix qui n'est presque jamais fait), sans leur donner de réel pouvoir sur le contenu du service et la manière dont leurs données sont traitées. Mettre le numérique au service des droits individuels, tel devrait être le premier principe directeur de la protection des droits fondamentaux dans les usages numériques. Par cette logique d'autonomisation des personnes (en anglais, « *empowerment* »), l'intervention publique peut accroître la capacité des individus à agir pour la défense de leurs droits et à amplifier ainsi les possibilités d'action des pouvoirs publics eux-mêmes. Face à des acteurs du numérique dont le succès passe par leur relation privilégiée avec leurs utilisateurs, les pouvoirs publics doivent, eux aussi, savoir « *s'allier avec la multitude* ».

Le second principe directeur des propositions formulées tend à mettre le numérique au service de l'intérêt général. Le numérique peut bénéficier de manière considérable à l'efficacité des politiques de santé, d'éducation, de culture, de sécurité ou de lutte contre la fraude, ainsi qu'à la simplification des démarches administratives ; encore faut-il que les personnes publiques disposent de cadres et d'instruments juridiques appropriés pour saisir ces opportunités, tout en assurant le respect des droits individuels. Il s'agit pour elles de concilier des droits fondamentaux entre eux ou des libertés avec des objectifs de valeur constitutionnelle, comme par exemple la sûreté à laquelle concourent la prévention et la répression des infractions les plus graves.

Même s'il reste un espace d'action autonome pour le droit interne, soit par la norme législative ou réglementaire, soit par le droit souple, nombre des propositions de cette étude relèvent de la compétence des institutions de l'Union européenne, soit parce qu'elles nécessitent une modification du droit de l'Union existant, soit parce que l'Union européenne constitue le niveau pertinent d'action.

1.1. Définir les principes fondant la protection des droits fondamentaux à l'ère du numérique

Il est parfois proposé de reconnaître aux personnes un véritable droit de propriété sur leurs données, en pariant sur leur plus grande implication du fait

qu'elles deviendraient financièrement intéressées à une bonne gestion de leurs données. Le Conseil d'État ne recommande pas une telle orientation. S'il préconise de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant ce dernier comme un *droit à l'autodétermination* plutôt que comme un droit de propriété (proposition n° 1). Car la reconnaissance du droit de propriété ne permettrait pas de rééquilibrer la relation entre les individus et les acteurs économiques et compliquerait l'exercice de la régulation par les pouvoirs publics. En effet, d'une part, le rapport de force entre l'individu, propriétaire de ses données, et l'entreprise resterait marqué par un déséquilibre structurel. D'autre part, si un droit de propriété était reconnu, il serait plus difficile au législateur d'imposer au droit de propriété des limites qui sont pourtant utiles à la vie en société : fichiers de police, de sécurité sociale, de l'administration fiscale etc. Le droit à « *l'autodétermination informationnelle* », concept dégagé par la Cour constitutionnelle allemande en 1983, est, à la différence du droit de propriété, un droit attaché à la personne tendant à « *garantir en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* ». Ce droit ne devrait pas être défini comme un droit supplémentaire s'ajoutant aux autres droits (droit d'information, droit d'accès, etc.), mais comme un principe donnant sens à tous ces droits, ceux-ci tendant à le garantir et devant être interprétés et mis en œuvre à la lumière de cette finalité.

Le principe de neutralité des opérateurs de communications électroniques doit être inscrit dans le droit positif, en prévoyant une définition large des services spécialisés assortie de pouvoirs importants des autorités de régulation pour veiller au maintien de la qualité générale d'Internet (proposition n° 2). Les plateformes, qui constitueraient une nouvelle catégorie juridique, seraient quant à elles soumises à une obligation de loyauté, consistant 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 (proposition n° 3).

1.2. Renforcer les pouvoirs des personnes et de leurs groupements

Le renforcement des capacités d'action des individus doit intervenir à deux niveaux, individuel et collectif.

Au niveau individuel, l'étude du Conseil d'État préconise de :

- donner à la CNIL, et à l'ensemble des autorités de protection des données européennes, une mission explicite de promotion des technologies renforçant la maîtrise des personnes sur l'utilisation de leurs données (proposition n° 4) ;
- mettre en œuvre de manière efficace le droit au déréférencement reconnu par la CJUE dans son arrêt *Google Spain,* notamment en donnant aux éditeurs des sites, dont le déréférencement est demandé, la possibilité de faire valoir leurs observations et en explicitant par des lignes directrices des autorités de protection des données leur doctrine de mise en œuvre de l'arrêt (proposition n° 5) ;
- définir les obligations des plateformes envers leurs utilisateurs qui découlent du principe de loyauté : notamment, 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, et définition des critères de retrait de contenus licites en termes clairs, accessibles à tous et non discriminatoires (proposition n° 6).

- organiser un droit d'alerte en matière de protection des données personnelles, sur le fondement du droit d'alerte « *généraliste* » reconnu par la loi du 6 décembre 2013 pour tout crime ou délit (proposition n° 7).

Les propositions portant sur les actions collectives sont les suivantes :

- créer une action collective en matière de protection des données personnelles, permettant à certaines personnes morales agréées d'obtenir du juge une injonction de faire cesser des violations de la législation (proposition n° 8) ;
- rendre accessible à tous sur Internet *via* la CNIL toutes les déclarations et autorisations de traitements de données (proposition n° 9) ;
- développer la participation des utilisateurs des plateformes à l'élaboration des règles définissant les contenus pouvant être mis en ligne sur leur site (proposition n° 10) ;
- attribuer à la CNIL ou au Conseil national du numérique une mission permanente d'animation de la délibération collective sur les enjeux éthiques liés au numérique (proposition n° 11).

1.3. Redéfinir les instruments de la protection des droits fondamentaux et repenser le rôle des autorités publiques

• ***En matière de protection des données personnelles***

Le cadre juridique de la protection des données personnelles a été défini alors que la circulation des données et leur valeur économique restaient limitées. L'intervention publique doit aujourd'hui assurer, d'une part, la sécurisation juridique des usages des données car c'est un facteur de développement de l'économie numérique et, d'autre part, un encadrement plus étroit des traitements présentant les risques les plus importants.

Afin de sécuriser juridiquement les usages présentant des risques limités pour les droits fondamentaux, les actions suivantes sont préconisées :

- maintenir sans ambiguïté dans la proposition de règlement européen la liberté de réutilisation statistique des données personnelles, quelle que soit la finalité initiale de leur traitement, en prévoyant pour seule condition que cette réutilisation soit entourée de garanties d'anonymat appropriées (proposition n° 12) ;
- renforcer le rôle de conseil et d'accompagnement des responsables de traitement par la CNIL et créer auprès d'elle une procédure de *rescrit « données personnelles »*[206] (propositions n° 13 et 14) ;

206 V. sur ce thème, *Le rescrit : sécuriser les initiatives et les projets*, la documentation Française, coll. Les études du Conseil d'État, mars 2014.

- développer la corégulation avec les acteurs professionnels, en prévoyant une procédure d'homologation des codes de conduite, le respect d'un code homologué devant être l'un des critères retenus par l'autorité de contrôle pour ses décisions d'autorisation ou de sanction (propositions n° 16, 17 et 18).

Afin de proportionner l'encadrement au degré de risque du traitement, il convient :

- de créer pour les catégories de traitements présentant les risques les plus importants une obligation de certification périodique (complétant l'examen *a priori* par l'autorité de contrôle dans le cadre de la procédure de consultation préalable) par un organisme tiers indépendant et accrédité par l'autorité de contrôle (proposition n° 19) ;
- de porter une attention particulière aux transmissions de données personnelles d'une entité à une autre, notamment en codifiant dans la loi la jurisprudence relative à la nullité des transactions portant sur des fichiers non autorisés ou non déclarés à la CNIL (proposition n° 20).

Le régime juridique des numéros d'identification devrait être revu, en mettant à l'étude la création d'un numéro national non signifiant (proposition n° 21) et, dans l'immédiat, en élargissant les possibilités de recours au NIR[207] dans le domaine de la santé et pour les autres usages (proposition n° 22). Enfin, la protection des droits fondamentaux nécessite la mise en place d'outils de régulation de l'utilisation des algorithmes, notamment par l'exigence d'effectivité de l'intervention humaine dans le traitement des données (proposition n° 23) ou par l'observation de leurs résultats, notamment pour détecter des discriminations illicites, en renforçant à cette fin les moyens humains dont dispose la CNIL (proposition n° 25).

• ***En matière de liberté d'expression***

Il conviendrait de prévoir une obligation pour les hébergeurs et les plateformes d'empêcher, durant un délai déterminé, la réapparition des contenus ayant fait précédemment l'objet de retrait ; cette obligation serait prononcée par l'autorité administrative (proposition n° 28).

L'existence de modalités spécifiques de contrôle des concentrations, qui complètent le contrôle général opéré par l'Autorité de la concurrence, est une garantie importante du pluralisme des médias. Cependant, en raison de la surabondance des contenus, les principales menaces pesant sur le libre choix des destinataires ne tiennent plus seulement à une concentration excessive, mais aussi à la fragilisation du modèle économique de la presse, alors que celle-ci demeure une source essentielle d'information de qualité. Il conviendrait de revoir le contrôle de la concentration dans les médias et, notamment, les quotas et la mesure des bassins d'audience utilisés pour la limiter, propre à mieux garantir le pluralisme en tenant compte de la multiplicité des supports d'information (proposition n° 30).

207 NIR : numéro d'inscription au Répertoire National d'Identification des Personnes Physiques (RNIPP), dit « *numéro de sécurité sociale* ».

• ***Par le développement de la médiation***

Nombre de litiges liés à l'utilisation des technologies numériques, qu'ils portent sur les données personnelles, les atteintes à la réputation sur Internet ou le retrait de contenus mis en ligne, peuvent être qualifiés de *petits litiges* : leurs enjeux sont parfois significatifs pour les personnes concernées, mais les intérêts pécuniaires en cause sont le plus souvent limités. Les procédures juridictionnelles classiques sont peu adaptées au traitement de ces petits litiges, ce qui conduit nombre de personnes à renoncer à faire valoir leurs droits ; la médiation serait dans bien des cas plus adaptée (proposition n° 31).

1.4. Assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques

• ***En matière d'ouverture des données publiques***

L'ouverture des données publiques (en anglais, « *Open Data* »), fait l'objet depuis 2011 d'une politique volontariste du Gouvernement. Ce volontarisme politique, qui se traduit par l'affichage d'un principe d'ouverture par défaut, aujourd'hui inscrit dans un instrument de droit souple, contraste avec la faiblesse des obligations prévues par le droit dur. L'inscription dans la loi d'une obligation de mise en ligne progressive de l'ensemble des bases de données détenues par l'administration présenterait plusieurs avantages, notamment celui d'étendre la politique d'ouverture des données publiques aux collectivités territoriales, dont l'action en la matière est aujourd'hui inégale. Toutefois, la voie du droit souple apparaît plus appropriée pour promouvoir un tel développement, notamment auprès de ces dernières. Une charte d'engagements et de bonnes pratiques pourrait donc être élaborée par l'État, les associations de collectivités territoriales et les représentants des utilisateurs des données. Cette charte engagerait chaque organisme public adhérent à définir un programme d'ouverture de ses données publiques, à respecter des standards de qualité et à veiller à limiter les risques de réidentification (proposition n° 32). Ces risques seraient circonscrits par la définition de bonnes pratiques d'anonymisation et par la constitution, au sein de chaque ministère, d'un pôle d'expertise en matière d'anonymisation, *a priori* au sein du service statistique ministériel (proposition n° 33).

• ***En matière de fichiers de police judiciaire***

Les fichiers de police judiciaire ont connu au cours des quinze dernières années une forte expansion liée notamment à l'allongement de la liste des infractions donnant lieu à enregistrement. Sans remettre en cause leur utilité pour les services de police, il apparaît souhaitable de renforcer les garanties entourant leur utilisation et de corriger certaines fragilités juridiques :

- Pour le fichier automatisé des empreintes digitales (FAED) et le fichier national automatisé des empreintes génétiques (FNAEG), il conviendrait de préciser les conséquences à tirer des décisions judiciaires : acquittement, non-lieu, relaxe, classement sans suite (proposition n° 34). Pour le fichier « Traitement des antécédents judiciaires », il s'agit d'assurer la mise en œuvre effective des

dispositions qui le régissent (proposition n° 35), les contrôles successifs de la CNIL ayant montré un taux très élevé d'erreurs et l'absence de prise en compte des suites judiciaires.

- La décision n° 2010-25 QPC du 16 septembre 2010 du Conseil constitutionnel devrait être mise en œuvre, en modulant la durée de conservation des données dans le FNAEG en fonction de la gravité de l'infraction et de l'âge de la personne au moment de l'enregistrement (proposition n° 36).

• ***En matière de prévention des atteintes à la sécurité nationale***

Les conséquences de l'arrêt du 8 avril 2014 de la CJUE *Digital Rights Ireland* doivent être tirées en ce qui concerne l'accès aux données de connexion collectées au titre de l'obligation de conservation systématique prévue par notre législation, notamment en réservant l'accès à des fins de police judiciaire aux crimes et aux délits d'une gravité suffisante, en réexaminant les régimes prévoyant l'accès de certaines autorités administratives pour des finalités autres que la sécurité intérieure (notamment la HADOPI, l'ANSSI, l'administration fiscale, l'AMF) et en étendant, pour l'accès aux données de connexion, les règles spécifiques de protection qui bénéficient aux parlementaires, aux avocats, aux magistrats et aux journalistes en matière d'interceptions du contenu des communications (proposition n° 38).

Afin de satisfaire à l'exigence de prévisibilité de la loi issue de la jurisprudence de la CEDH, il conviendrait de définir par la loi le régime de l'interception des communications à l'étranger, en prévoyant les finalités de ces interceptions les garanties spécifiques bénéficiant aux résidents français et l'existence d'un contrôle d'une autorité administrative indépendante (proposition n° 39). Il conviendrait également de définir le régime juridique de l'utilisation par les services de renseignement, sur autorisation administrative, de certains moyens d'investigation spéciaux utilisant les techniques numériques aujourd'hui encadrés uniquement dans le cadre de la procédure judiciaire : déchiffrement, captation de données informatiques, etc. (proposition n° 40).

Il est proposé de faire de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) une autorité de contrôle des services de renseignement, dotée de moyens humains renforcés sur le plan quantitatif et qualitatif, avec des compétences de haut niveau en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données. Ses prérogatives devraient aussi être renforcées, par l'attribution de pouvoirs de contrôle sur pièces et sur place et d'un champ de compétences étendu aux interceptions opérées à l'étranger ainsi qu'à l'emploi des moyens d'investigations spéciaux (proposition n° 41). Les agents impliqués dans la mise en œuvre des programmes de renseignement auraient un droit de signalement à cette autorité administrative indépendante des pratiques manifestement contraires au cadre légal, selon des modalités sécurisées assurant la protection du secret de la défense nationale (proposition n° 42).

1.5. Organiser la coopération européenne et internationale

Un socle de règles applicables à tous les services dirigés vers l'Union européenne ou la France (selon que la règle est européenne ou nationale), quel que soit leur lieu d'établissement comprendrait (proposition n° 43) :

- la législation européenne relative à la protection des données personnelles, qui serait qualifiée à cette fin de « *loi de police* » au sens du droit international privé ;
- l'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judiciaires, prévue par l'article 6 de la loi pour la confiance dans l'économie numérique, dont le champ d'application territorial serait explicité ;
- le droit pénal, notamment les abus de la liberté d'expression, qui est déjà applicable à l'ensemble des sites, même établis à l'étranger mais destinés au public français.

En matière de protection des données personnelles, le « *Safe Harbor* » négocié avec les autorités américaines, devrait être réformé, en prévoyant un droit de regard des autorités européennes sur les contrôles et en renforçant les obligations de fond (proposition n° 44). En matière de lutte contre la cybercriminalité, un groupe d'action interétatique devrait être créé pour définir des recommandations et publier une liste d'États non coopératifs (proposition n° 47).

L'annonce de la fin du lien contractuel entre la Société pour l'attribution des noms de domaine et des numéros sur Internet (en anglais, « *Internet Corporation for Assigned Names and Numbers* » ou ICANN) et le gouvernement américain ouvre des perspectives de réforme de la gouvernance d'Internet, pour l'ICANN mais aussi pour les autres instances qui doivent être investies d'une mission d'intérêt général guidée par un *mandat international*. Le processus de réforme en cours doit être l'occasion de donner une traduction concrète à ces exigences. Il conviendrait de promouvoir la démocratisation de l'ICANN, notamment en créant une assemblée générale rassemblant l'ensemble des parties prenantes et pouvant mettre en cause la responsabilité du conseil d'administration. Le rôle des États devrait être renforcé, en permettant au comité représentant les gouvernements (GAC) d'adopter des résolutions contraignantes (proposition n° 48). Pour l'ensemble des instances, il conviendrait de diversifier la composition des organes de gouvernance d'Internet par des critères de sélection imposant une réelle diversité linguistique et géographique et la mise en place de stratégies d'influence de la France et de l'Union européenne (proposition n° 49). Une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'Internet devrait notamment énoncer les principes que s'imposeraient les signataires (proposition n° 50).

2. Récapitulatif des mesures proposées

Définir les principes fondant la protection des droits fondamentaux à l'ère du numérique (3.1.)

Le droit sur les données personnelles : un droit à l'autodétermination plutôt qu'un droit de propriété (3.1.1.)

Proposition n° 1

Concevoir le droit à la protection des données personnelles comme un droit à « *l'autodétermination informationnelle* », c'est-à-dire le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel.

Inscrire cette conception dans la proposition de règlement relatif à la protection des données à caractère personnel ou, dans l'attente du règlement, dans la loi du 6 janvier 1978.

Ne pas faire entrer les données personnelles dans le champ du droit de propriété patrimonial des personnes.

Vecteur : règlement de l'Union européenne ou loi.

Neutralité des réseaux, loyauté des plateformes (3.1.2.)

Proposition n° 2

Consacrer le principe de neutralité des opérateurs de communications électroniques dans les termes votés par le Parlement européen le 3 avril 2014, sous trois réserves :

- Revenir à la définition des mesures de gestion de trafic de la proposition de la Commission ;

- Revenir à la définition plus large des « services spécialisés », mais avec des contreparties : information préalable de l'autorité de régulation concernée sur le projet de convention ; droit d'opposition si risque manifeste de dégradation de la qualité de l'internet en-deçà d'un niveau satisfaisant ; droit de suspension de l'autorité de régulation s'il s'avère que qualité de l'internet est dégradée ;

- Droit des opérateurs d'exiger un paiement des fournisseurs de contenus, dans le cadre d'une facturation asymétrique, lorsqu'ils représentent à eux seuls une part significative du trafic.

Vecteur : loi ou règlement de l'Union européenne.

Proposition n° 3

Définir la catégorie juridique des plateformes, distincte de celle des simples hébergeurs passifs. 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. Les plateformes seraient soumises à un principe de loyauté.

Vecteur : directive de l'Union européenne.

Renforcer les pouvoirs des individus et de leurs groupements (3.2.)

Renforcer les capacités d'action individuelle (3.2.1.)

Proposition n° 4

Donner à la CNIL et à l'ensemble des autorités de protection des données européennes une mission explicite de promotion des technologies renforçant la maîtrise des personnes sur l'utilisation de leurs données.

Envisager notamment les actions suivantes :

- Lancer au niveau européen une concertation multiacteurs dans le but de susciter l'émergence des solutions technologiques les plus prometteuses en termes de renforcement de la vie privée ;

- Promouvoir la diffusion gratuite d'outils de renforcement de la vie privée par les FAI, soit dans un cadre volontaire, soit en l'imposant par la loi comme c'est le cas pour les logiciels de contrôle parental ;

- Dans le cadre de la standardisation des politiques d'utilisation des données personnelles prévue par le projet de règlement européen, susciter le développement de règlements-types définissant des polices d'utilisation, auxquels un grand nombre d'internautes adhéreraient et que les entreprises seraient donc conduites à prendre en compte pour définir leur propre politique.

- Développer l'intervention de prestataires « *tiers de confiance* », afin de garantir que seules les données dont la personne a autorisé la divulgation sont diffusées.

Vecteur : Loi, règlement de l'Union européenne, action de la CNIL et des autres autorités européennes de protection des données.

Proposition n° 5

Mettre en œuvre de manière efficace le droit au déréférencement consacré par l'arrêt *Google Spain*, en :

- Donnant aux éditeurs des sites dont le déréférencement est demandé la possibilité de faire valoir leurs observations ;

- Explicitant par des lignes directrices la doctrine de mise en œuvre de *Google Spain* par les autorités de protection des données ;

- Organisant les conditions d'une décision unique de déréférencement, soit par accords de reconnaissance mutuelle des décisions de déréférencement prises par les exploitants de moteurs de recherche, soit par un dispositif légal d'extension à tous les exploitants d'une décision prise par l'un d'entre eux, sous réserve de son homologation par un juge.

Vecteur : lignes directrices du G29 pour les deux premiers points ; accord entre les exploitants de moteurs de recherche ou loi pour le troisième.

Proposition n° 6

Définir les obligations des plateformes envers leurs utilisateurs, 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 ;

- mettre l'utilisateur ayant mis en ligne un contenu en mesure de faire valoir ses observations en cas de retrait de celui-ci ;

- en ce qui concerne les utilisateurs commerciaux, notification préalable, avec un délai de réponse raisonnable, des changements de la politique de contenus ou de l'algorithme susceptibles d'affecter le référencement ou le classement.

Vecteur : directive de l'Union européenne ou droit souple (chartes d'engagements des plateformes)

Proposition n° 7

Mettre en œuvre le droit d'alerte pour les salariés des organismes traitant des données personnelles, par des processus d'information et de déclaration placés sous la responsabilité de la CNIL.

Vecteur : action de la CNIL.

Renforcer les capacités d'action collective (3.2.2.)

Proposition n° 8

Créer une action collective, distincte de l'action de groupe, destinée à faire cesser les violations de la législation sur les données personnelles. Cette action serait exercée devant le tribunal de grande instance par les associations agréées de protection de consommateurs ou de défense de la vie privée et des données personnelles.

Vecteur : loi.

Proposition n° 9

Mettre en *Open Data* toutes les déclarations et autorisations de traitements de données.

Vecteur : action de la CNIL.

Dans le cadre du projet de règlement européen, prévoir la publication sur le site de l'autorité de protection des données par les délégués à la protection des données, d'un rapport d'information annuel sur les traitements mis en œuvre par leur organisme.

Vecteur : règlement de l'Union européenne.

Proposition n° 10

Développer la participation des utilisateurs des plateformes à l'élaboration des règles définissant les contenus pouvant être mis en ligne sur leur site.

Vecteur : droit souple (charte d'engagements des plateformes) ; recommandations de l'autorité de régulation compétente.

Proposition n°11

Confier à la CNIL ou au Conseil national du numérique une mission permanente d'animation de la délibération collective sur les enjeux éthiques liés au numérique.

Vecteur : loi pour la CNIL, décret pour le CNNum.

Redéfinir les instruments de la protection des droits fondamentaux et repenser le rôle des autorités publiques (3.3.)

Tirer les conséquences du passage à l'ère de l'économie des données personnelles (3.3.1.)

Proposition n° 12

Afin de sécuriser le développement du *Big Data* en Europe, maintenir sans ambiguïté dans la proposition de règlement européen la liberté de réutilisation statistique des données personnelles, quelle que soit la finalité initiale de leur traitement, en prévoyant pour seule condition que cette réutilisation soit entourée de garanties d'anonymat appropriées.

Vecteur : le règlement de l'Union européenne

Proposition n° 13

Renforcer le rôle de conseil et d'accompagnement des responsables de traitement par la CNIL.

Vecteur : action de la CNIL.

Proposition n° 14

Créer un *certificat de conformité (rescrit « données personnelles »*).

Vecteur : loi.

Proposition n° 15

Clarifier le champ des traitements soumis en raison de leurs risques à des obligations particulières telles que la réalisation d'une étude d'impact ou la consultation préalable de l'autorité de contrôle, en définissant dans le règlement la liste des catégories de traitement concernées. La soumission à l'obligation de consultation préalable ne doit pas dépendre du résultat de l'étude d'impact.

Vecteur : règlement de l'Union européenne.

Proposition n° 16

Créer une procédure d'homologation des codes de conduite professionnels élaborés au niveau national ou européen.

Vecteur : règlement de l'Union européenne.

Proposition n° 17

Développer la normalisation en matière de sécurité des traitements de données personnelles.

Vecteur : règlement de l'Union européenne.

Proposition n° 18

Participer et organiser la transition vers le nouveau cadre juridique issu du règlement, par une coopération entre le gouvernement, la CNIL et les principaux acteurs professionnels concernés.

Vecteur : action du gouvernement, de la CNIL et des principaux acteurs professionnels concernés.

Proposition n° 19

Créer pour les catégories de traitements présentant les risques les plus importants une obligation de certification périodique (complétant l'examen *a priori* par l'autorité de contrôle dans le cadre de la procédure de consultation préalable) par un organisme tiers indépendant et accrédité par l'autorité de contrôle.

Vecteur : règlement de l'Union européenne.

Proposition n° 20

Porter une attention particulière aux transmissions de données personnelles d'une entité à une autre en :

- codifiant dans la loi la jurisprudence relative à la nullité des transactions portant sur des fichiers non déclarés ou non autorisés à la CNIL (*vecteur : loi*) ;

- incitant les acteurs procédant de manière récurrente à de telles transactions à en tenir un registre (*vecteur : code de conduite professionnel*) ;

- incitant à fournir aux personnes exerçant leur droit d'accès une liste complète des entités auxquelles leurs données ont été communiquées (*vecteur : code de conduite professionnel*).

Proposition n° 21

Mettre à l'étude la création d'un numéro national unique d'identification non signifiant.

Vecteur : action du Gouvernement et de la CNIL.

Proposition n° 22

Permettre le recours au NIR pour les traitements de données personnelles ayant pour fin la recherche dans le domaine de la santé et autorisés par la CNIL en vertu du chapitre IX de la loi du 6 janvier 1978. Admettre l'utilisation du NIR comme identifiant national pour les données de santé.

Vecteur : loi ; action de la CNIL.

Définir un droit des algorithmes prédictifs (3.3.2.)

Proposition n° 23

Pour assurer l'effectivité de l'interdiction de fonder une décision sur la seule mise en œuvre d'un traitement automatisé, confirmer que l'intervention humaine dans la décision doit être réelle et pas seulement formelle. Indiquer dans un instrument de droit souple les critères d'appréciation du caractère effectif de l'intervention humaine.

Vecteur : règlement de l'Union européenne et droit souple (recommandation de la CNIL ou avis du G29).

Proposition n° 24

Imposer aux auteurs de décisions s'appuyant sur la mise en œuvre d'algorithmes une obligation de transparence sur les données personnelles utilisées par l'algorithme et le raisonnement général suivi par celui-ci.

Donner à la personne faisant l'objet de la décision la possibilité de faire valoir ses observations.

Vecteur : loi ou règlement de l'Union européenne.

Proposition n° 25

Dans le cadre de l'article 44 de la loi du 6 janvier 1978, et dans le respect du secret industriel, développer le contrôle des algorithmes par l'observation de leurs résultats, notamment pour détecter des discriminations illicites, en renforçant à cette fin les moyens humains dont dispose la CNIL.

Vecteur : action de la CNIL.

Proposition n° 26

Analyser les pratiques de différenciation des prix reposant sur l'utilisation des données personnelles, mesurer leur développement et déterminer celles qui devraient être qualifiées de pratiques commerciales illicites ou déloyales, et sanctionnées comme telles.

Vecteur : action de la DGCCRF ; saisine du Conseil national de la consommation de l'Autorité de la concurrence ; loi à l'issue de la réflexion.

Proposition n° 27

Encourager la prise en compte de la diversité culturelle dans les algorithmes de recommandation utilisés par les sites internet diffusant des contenus audiovisuels ou musicaux.

Vecteur : droit souple ou conventions conclues avec le CSA.

Organiser la répartition des rôles entre acteurs publics et acteurs privés dans la lutte contre les contenus illicites (3.3.3.)

Proposition n° 28

Aligner le régime de responsabilité civile et pénale des plateformes sur celui des hébergeurs. Prévoir une obligation pour les hébergeurs et les plateformes d'empêcher, durant un délai déterminé, la réapparition des contenus ayant fait précédemment l'objet de retrait. Cette obligation serait prononcée par l'autorité administrative.

Vecteur : loi (pour les plateformes, après l'intervention de la directive de l'Union européenne créant la catégorie juridique des plateformes).

Proposition n° 29

Encadrer l'utilisation des outils de surveillance automatique des contenus mis en œuvre volontairement par les plateformes en prévoyant une obligation de transparence sur l'utilisation de ces outils, leur fonctionnement et l'étendue des blocages de contenus qu'ils entraînent.

Vecteur : loi (après l'intervention de la directive de l'Union européenne créant la catégorie juridique des plateformes).

Adapter les instruments de la promotion du pluralisme des médias (3.3.4.)

Proposition n° 30

Revoir le contrôle de la concentration dans les médias, et notamment les quotas de diffusion et la mesure des bassins d'audience utilisés pour la limiter, afin de mieux garantir le pluralisme au regard de l'ensemble des modes de diffusion contemporains.

Vecteur : concertation en vue d'une loi.

Développer la médiation pour régler les litiges liés à l'utilisation des technologies numériques (3.3.5.)

Proposition n° 31

Mettre en place un système de médiation facilement accessible pour régler les petits litiges entre personnes privées liés à l'utilisation des technologies numériques, tels que ceux concernant les données personnelles, les atteintes à la réputation sur internet ou le retrait de contenus mis en ligne.

Vecteur : accord entre les parties prenantes ou loi.

Assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques (3.4.)

Poursuivre l'ouverture des données publiques tout en prévenant les risques pour la vie privée (3.4.1.)

Proposition n° 32

Afin de promouvoir le développement de l'*open data* auprès des personnes publiques, notamment les collectivités territoriales :

- Adopter une charte d'engagements et de bonnes pratiques signée par l'État, les associations de collectivités territoriales et les représentants des utilisateurs des données publiques, et promouvoir l'adhésion des personnes publiques à cette charte.

- Accroître le rôle d'appui des services de l'État aux collectivités territoriales souhaitant ouvrir leurs données publiques

Vecteur : droit souple (charte d'engagements et de bonnes pratiques) et décret.

Proposition n° 33

Pour les données publiques comportant des données personnelles, maîtriser les conditions de leur ouverture afin de limiter étroitement le risque de réidentification.

À cette fin :

- Faire définir par la CNIL, en concertation étroite avec le comité du secret statistique et la CADA, des standards d'anonymisation ;

- Constituer au sein de chaque ministère un pôle d'expertise en matière d'anonymisation, *a priori* au sein du service statistique ministériel ;

- Assurer l'accessibilité de ces services d'expertise aux collectivités territoriales qui en font la demande auprès du préfet.

- Lorsque le risque de réidentification ne peut être écarté, définir une procédure d'accès sur autorisation plutôt que de mettre en ligne, en particulier lorsque sont en cause des données sensibles (par exemple des données de santé, des données fiscales ou des informations sur les difficultés sociales des personnes).

Vecteur : Droit souple (recommandations de bonnes pratiques) et organisation des services de l'État. Le cas échéant, dispositions législatives pour définir les procédures d'accès sur autorisation.

Renforcer les garanties entourant l'usage des fichiers de police (3.4.2.)

Proposition n° 34

Préciser, en s'inspirant des dispositions relatives au fichier « *Traitements d'antécédents judiciaires* » (TAJ), les conséquences à tirer des décisions judiciaires (classement sans suite, non-lieu, relaxe et acquittement) quant à l'effacement des données relatives aux personnes mises en cause, pour le fichier automatisé des empreintes digitales (FAED) et le fichier national automatisé des empreintes génétiques (FNAEG).

Vecteur : décret pour le FAED, loi pour le FNAEG.

Proposition n° 35

Définir un plan d'apurement des erreurs et insuffisances du fichier « *Traitements d'antécédents judiciaires* » (TAJ), notamment sur les suites judiciaires données aux mises en cause, afin de mettre à jour l'ensemble des fiches qui y sont contenues.

Vecteur : action du ministère de la justice et du ministère de l'intérieur.

Proposition n° 36

Mettre en œuvre la décision n° 2010-25 QPC du 16 septembre 2010 du Conseil constitutionnel, en modulant la durée de conservation des données dans le fichier national automatisé des empreintes génétiques (FNAEG) en fonction de la gravité de l'infraction et de la minorité de la personne au moment de l'enregistrement.

Vecteur : décret en Conseil d'État.

Proposition n° 37

Définir un régime d'autorisation aux formalités allégées (spécifications du traitement moins précises et autorisation délivrée par la CNIL dans le cadre de l'article 25 de la loi du 6 janvier 1978) pour les expérimentations de traitements de données régis par les articles 26 et 27 de la loi du 6 janvier 1978.

Vecteur : loi.

Conjuguer le plein respect des droits fondamentaux et l'efficacité de la surveillance des communications électroniques à des fins de renseignement (3.4.3.)

Proposition n° 38

Tirer les conséquences de l'arrêt *Digital Rights Ireland* en ce qui concerne l'accès aux métadonnées, en :

- réservant l'accès à des fins de police judiciaire aux crimes et aux délits d'une gravité suffisante ;

- réexaminant les régimes prévoyant l'accès de certaines autorités administratives pour des finalités autres que la sécurité intérieure (par exemple HADOPI, ANSSI, administration fiscale, AMF), et notamment les circonstances dans lesquelles cet accès peut être demandé et les données peuvent être communiquées ;

- modulant la période accessible en fonction de la finalité et de la gravité des infractions ;

- étendant, pour l'accès aux métadonnées, les règles spécifiques de protection qui bénéficient aux parlementaires, aux avocats, aux magistrats et aux journalistes.

Vecteur : loi.

Proposition n° 39

Définir par la loi le régime de l'interception des communications à l'étranger. La loi déterminerait les finalités de ces interceptions et habiliterait l'Autorité de contrôle des services de renseignement à exercer son contrôle sur ces activités.

Vecteur : loi.

Proposition n° 40

Définir le régime juridique de l'utilisation par les services de renseignement, sur autorisation administrative, de certains moyens d'investigation spéciaux prenant appui sur des techniques numériques (déchiffrement, captation de données informatiques...).

Vecteur : loi.

Proposition n° 41

Faire de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) une Autorité de contrôle des services de renseignement dotée de moyens et de prérogatives renforcés.

Vecteur : loi.

Proposition n° 42

Créer un droit de signalement à l'Autorité de contrôle des services de renseignement, l'ACSR, permettant aux agents impliqués dans la mise en œuvre des programmes de renseignement de signaler des pratiques manifestement contraires au cadre légal. Ce droit de saisine serait effectué selon des modalités sécurisées assurant la protection du secret de la défense nationale.

Vecteur : loi.

Organiser la coopération européenne et internationale (3.5.)

Affirmer l'applicabilité du droit européen et organiser la coopération au sein de l'Union européenne (3.5.1.)

Proposition n° 43

Définir un socle de règles applicables à tous les services dirigés vers l'Union européenne ou la France (selon que la règle est européenne ou nationale), quel que soit leur lieu d'établissement. Ce socle comprendrait :

- la législation européenne relative à la protection des données personnelles, qui serait qualifiée à cette fin de « *loi de police* » au sens du droit international privé.

- l'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judiciaires, prévue par l'article 6 de la LCEN, dont le champ d'application territorial serait explicité.

- le droit pénal, qui est déjà applicable à l'ensemble des sites destinés au public français.

Vecteur : règlement de l'Union européenne pour la protection des données personnelles / loi pour l'obligation de coopération des hébergeurs et des plateformes.

Promouvoir de nouvelles formes de coopération avec les autres espaces juridiques (3.5.2.)

Proposition n° 44

Réformer le *Safe Harbor* en développant les contrôles par la *Federal Trade Commission* américaine (FTC) ou des organismes accrédités par elle, en prévoyant un droit de regard des autorités européennes sur ces contrôles et en renforçant les obligations de fond.

Vecteur : décision de la Commission européenne.

Proposition n° 45

Prévoir que les transferts de données personnelles vers certains État tiers, lorsqu'ils sont requis par les autorités administratives ou judiciaires de cet État, sont subordonnés à l'autorisation préalable de l'autorité de contrôle compétente. La décision d'appliquer ce régime à un État tiers, prise par la Commission, est temporaire et renouvelable ; elle doit être justifiée par le non-respect des standards de l'État de droit ou par le caractère excessif des pratiques de collecte de renseignement.

Vecteur : règlement de l'Union européenne.

Proposition n° 46

Subordonner la reconnaissance par l'UE du caractère adéquat de la protection dans des États tiers à une condition de réciprocité.

Vecteur : action de la Commission européenne

Proposition n° 47

Créer un groupe d'action interétatique, sur le modèle du Groupe d'action financière (GAFI), pour définir des recommandations en matière de lutte contre la cybercriminalité et publier une liste d'États non coopératifs.

Vecteur : action du Conseil de l'Europe

Rééquilibrer la gouvernance d'internet (3.5.3.)

Proposition n° 48

Promouvoir la démocratisation de l'ICANN, en :

- créant une assemblée générale rassemblant l'ensemble des parties prenantes et pouvant mettre en cause la responsabilité du conseil d'administration ;

- renforçant les mécanismes de recours internes, par exemple en dotant d'une portée contraignante le mécanisme d'*Independent Review Panel* ;

- permettant au comité représentant les gouvernements (GAC) d'adopter des résolutions contraignantes.

Vecteur : modification des statuts de l'ICANN.

Proposition n° 49

Diversifier la composition des instances de gouvernance d'internet, par des critères de sélection imposant une réelle diversité linguistique et géographique et la mise en place de stratégies d'influence au niveau de la France et de l'Union européenne.

Vecteur : modification des statuts de ces instances, action du Gouvernement français et de l'Union européenne.

Proposition n° 50

Promouvoir l'adoption d'une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet.

Vecteur : convention internationale.

Annexe 2 : Sélection de textes et de jurisprudences

1. Sélection de textes

1.1. Droit européen

Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens, n° 108.

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, *JOUE* n° L 281 du 23 novembre 1995 p. 31.

Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (directive « sur le commerce électronique »), *JOUE* n° L 178 du 17/07/2000 p. 0001 – 0016.

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 relative au traitement de données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques, *JOUE*, n° L 201 du 31/07/2002, p. 37 (Modifiée par la 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, *JOUE*, n° L. 337 du 18 décembre 2009, p. 11.

Projet de règlement européen du 25 janvier 2012 relatif aux données personnelles. Destiné à réformer la directive de 1995 (95/46/CE) sur la protection des données, le futur règlement européen inclut des mesures de protection des données personnelles des citoyens, et limite l'utilisation de ces données par les services de renseignements et les entreprises. Il s'applique à tous les traitements de données personnelles effectués sur le territoire de l'Union européenne, que le responsable du traitement soit physiquement implanté en Europe ou non. Son adoption est prévue pour 2016. Un projet de directive complètera ce règlement aux fins d'améliorer la coopération judiciaire entre les États européens et la poursuite des effractions constatées.

1.2. Droit national

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (*JORF*, 7 janvier 1978, p. 227) **modifiée** 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 (*JORF*, 7 août 2004, p. 14063) et par la loi n° 2014-344 du 17 mars 2014 relative à la consommation.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (*JORF* n° 0143, 22 juin 2004, page 11168, texte n° 2).

2. Sélection de jurisprudences

2.1. Juridictions étrangères

Cour suprême des États-Unis

Katz c/ États-Unis, (1967), 389 U.S. 347, p. 361.

Miller v. United States, (1976), 425 U.S. 435.

Smith c/ Maryland, (1979), 442 U.S. 735.

Attorney general of the United States vs American Civil Liberties Union (ACLU) du 26 juin 1997.

Kyllo c/ États-Unis, (2000), 533, U.S. 141.

Krottner v. Starbucks Corp., (2010), 628 F.3d 1139, 1140.

Klayman e.a./Obama e.a., (2013), 13-0851.

Verizon vs FCC, (2014), n° 11-1355.

Cour constitutionnelle Fédérale d'Allemagne

Cour constitutionnelle fédérale d'Allemagne, 15 décembre 1983, *BVerfGE 65* (Arrêt sur le recensement, « *Volkszählungsurteil* » ; extrait cité dans le guide sur la protection des données dans les structures d'accueil de jour pour jeunes enfants, ministère de la Culture, de la Jeunesse et des Sports du *Land* de Bade-Wurtemberg).

> « *Quiconque n'est pas en mesure d'estimer avec une sécurité suffisante à qui sont divulguées les informations le concernant dans certains domaines de son environnement social et n'est pas capable d'évaluer approximativement ce que savent les partenaires de communication potentiels, peut voir sa liberté de planification et de décision de sa propre autodétermination considérablement inhibée. Un ordre social et juridique dans lequel le citoyen ne sait plus qui sait quoi et quant à son sujet, ni dans quelle situation, est incompatible avec le droit à l'autodétermination informationnelle. Une personne qui ne sait pas si tous ses comportements inhabituels sont consignés et enregistrés de façon permanente, utilisés ou diffusés, essaiera de ne pas attirer l'attention en adoptant ce type de comportement. (...) Cela limiterait non seulement les possibilités d'épanouissement personnel de l'individu, mais aussi le bien commun dans la mesure où l'autodétermination est une condition essentielle à l'existence d'une société libre et démocratique qui repose sur les capacités et la solidarité de ses citoyens. C'est pourquoi : le libre épanouissement de la personnalité suppose, dans les conditions modernes du traitement des données, la protection de l'individu contre la collecte, l'enregistrement, l'utilisation et la transmission illimitée de ses données personnelles. Cette protection se compose du droit fondamental de l'article 2, section 1, associé à l'article 1, section 1, de la loi fondamentale allemande (GG). Le droit fondamental garantit sur ce point le pouvoir de l'individu de décider lui-même de la divulgation et de l'utilisation de ses données personnelles. (...) Si l'individu 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* ».

Tribunal fédéral suisse

Tribunal fédéral suisse, 31 mai 2012, *Google Inc. et Google Switzerland S.A.R.L. c. préposé fédéral à la protection des données et à la transparence*, 1C_230/2011.

2.2. Juridictions européennes

CJCE / CJUE

CJCE, aff. C-325/85, 15 décembre 1987, *Irlande c/ Commission*, C-325/85.

CJCE, aff. C-262/88, 17 mai 1990, *Barber.*

CJCE, aff. C-7/97 26 novembre 1998, *Oscar Bronner c/ Mediaprint.*

CJCE, aff. C-101/01, 6 novembre 2003, *Bodil Lindqvist.*

CJCE, Gde Ch., aff. C-275/06, 29 janvier 2008, *Promusicae c/ Telefonica.*

CJUE, aff. C-236/08, Gde Ch., 23 mars 2010, *Google France et Google Inc c/ Louis Vuitton Malletier.*

CJUE, aff. C-92/09 et C-93/09, Gde Ch., 9 novembre 2010, *Volcker und Markus Schecke GbR et Hartmut Eifert.*

CJUE, aff. C-858/08, Gde Ch., 7 décembre 2010, *Pammer et Hotel Apenhof.*

CJUE, aff. C-324/09, Gde Ch., 12 juillet 2011, *L'Oréal c/ eBay*.

CJUE, Gde Ch., 25 octobre 2011, *eDate Advertising.*

CJUE, aff. C-70-10, 24 novembre 2011, *Scarlet c/ SABAM.*

CJUE, aff. C-360/10, 16 février 2012, *SABAM.*

CJUE, aff. C-523/10, 19 avril 2012, *Wintersteiger.*

CJUE, aff. C-617/10, Gde Ch., 26 février 2013, *Åklagaren c/ Hans Åkerberg Fransson.*

CJUE, aff. C-170/12, 3 octobre 2013, *Pinckney c/ Mediatech.*

CJUE, aff. C-314/12, 27 mars 2014, *UPC Telekabel*.

CJUE, Gde Ch., aff. C-293/12 et C-594/12, 8 avril 2014, *Digital Rights Ireland e. a. et Michael Seitlinger e. a.*

> « *(...) Sur l'existence d'une ingérence dans les droits consacrés par les articles 7 et 8 de la Charte.*
>
> « *32 En imposant la conservation des données énumérées à l'article 5, paragr. 1, de la directive 2006/24 et en permettant l'accès des autorités nationales compétentes à celles-ci, cette directive déroge, ainsi que l'a relevé M. l'avocat général, notamment aux points 39 et 40 de ses conclusions, au régime de protection du droit au respect de la vie privée, instauré par les directives 95/46 et 2002/58, à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques ; ces dernières directives ayant prévu la confidentialité des communications et des données relatives au trafic ainsi que l'obligation d'effacer ou de rendre anonymes ces données lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, hormis si elles sont nécessaires à la facturation et uniquement tant que cette nécessité perdure.*

« *33 Pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence (voir, en ce sens, l'arrêt* Österreichischer Rundfunk e.a.*, aff. C-465/00, C-138/01 et C-139/01, EU:C:2003:294, paragr. 75).*

« *34 Il en résulte que l'obligation imposée par les articles 3 et 6 de la directive 2006/24 aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications, telles que celles visées à l'article 5 de cette directive, constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte.*

« 35 *En outre, l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental (voir, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH,* Leander c. Suède*, 26 mars 1987, série A n° 116, paragr. 48 ;* Rotaru c. Roumanie *[GC], n° 28341/95, paragr. 46, CEDH 2000-V, ainsi que* Weber et Saravia c. Allemagne *(déc.), n° 54934/00, paragr. 79, CEDH 2006-XI). Ainsi, les articles 4 et 8 de la directive 2006/24 prévoyant des règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits garantis par l'article 7 de la Charte.*

« 36 *De même, la directive 2006/24 est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte puisqu'elle prévoit un traitement des données à caractère personnel.*

« 37 *Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave. En outre, la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.*

« *(…) Par ces motifs, la Cour (grande chambre) dit pour droit :*

« *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, est invalide ».*

CJUE, Gde Ch., aff. C-131/12, 13 mai 2014, *Google Spain c/ AEPD*.

« *(…) Par ces motifs, la Cour (grande chambre) dit pour droit :*

« 1) *L'article 2, sous b) et d), 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, doit être interprété en ce sens que, d'une part, l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de «* traitement de données à caractère personnel *», au sens de cet article 2, sous b), lorsque ces informations contiennent des données à caractère personnel et, d'autre part, l'exploitant de ce moteur de recherche doit être considéré comme le «* responsable *» dudit traitement, au sens dudit article 2, sous d).*

« 2) *L'article 4, paragr. 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre.*

« 3) *Les articles 12, sous b) et 14, premier alinéa, sous a), de la directive 95/46 doivent être interprétés en ce sens que, afin de respecter les droits prévus à ces dispositions et pour autant que les conditions prévues par celles-ci sont effectivement satisfaites, l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite.*

« 4) *Les articles 12, sous b) et 14, premier alinéa, sous a), de la directive 95/46 doivent être interprétés en ce sens que, dans le cadre de l'appréciation des conditions d'application de ces dispositions, il convient notamment d'examiner si la personne concernée a un droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne. Cette dernière pouvant, eu égard à ses droits fondamentaux au*

titre des articles 7 et 8 de la Charte, demander que l'information en question ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats, ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question ».

CEDH

CEDH Plénière, 6 septembre 1978, *Klass et autres c/ Allemagne,* n° 5029/71.
CEDH, 26 mars 1987, *Leander c/ Suède*, n° 9248/81.
CEDH, 24 avril 1990, *Kruslin c/ France*, n° 18801/85.
CEDH, 16 décembre 1992, *Niemetz c/ Allemagne*, n° 13710/88.
CEDH, Gde Ch., 11 janvier 2007, *Anheuser-Busch c/ Portugal*, n° 73049/01.
CEDH, 7 janvier 2008, *Jankovskis c/ Lituanie*, n° 21575/08.
CEDH, 1er juillet 2008, *Liberty et autres c/ Royaume-Uni*, n° 58243/00.
CEDH, Gde Ch., 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, n° 30562/04 et 305566/04.
CEDH, 16 juillet 2009, *Willem c/ France*, n° 10883/05.
CEDH, 16 juillet 2009, *Féret c/ Belgique*, n° 15615/07.
CEDH, 29 mars 2010, *Medvedyev c/ France*, n°3394/03.
CEDH, 18 mai 2010, *Kennedy c/ Royaume-Uni* , n° 26839/05.
CEDH, 2 septembre 2010, *Uzun c/ Allemagne*, n° 35623/05.
CEDH, 23 novembre 2010, *Moulin c/ France*, n° 37104/06.
CEDH, Gde Ch., 13 juillet 2012, *Mouvement raëlien suisse c/ Suisse*, n° 16354/06.
CEDH, 18 décembre 2012, *Yildirim c/ Turquie*, n° 3111/10.
CEDH, 18 avril 2013, *M.K. c/ France*, n° 19522/09.

CEDH, 18 septembre 2014, *Brunet c/ France*, n° 21010/10

L'existence de l'ingérence

« 1. *La Cour constate d'emblée que l'inscription au Système de traitement des infractions constatées (STIC) des données relatives au requérant a constitué une ingérence dans son droit à la vie privée, ce qui n'est pas contesté par le Gouvernement ».*

La justification de l'ingérence

a) Base légale et but légitime

« 2. *La Cour observe que cette ingérence était «* prévue par la loi *» et qu'elle poursuivait les «* buts légitimes *» de défense de l'ordre, de prévention des infractions pénales, et de protection des droits d'autrui ».*

b) Nécessité de l'ingérence

i. Les principes généraux

« 3. *Il lui reste donc à examiner la nécessité de l'ingérence au regard des exigences de la Convention, qui commandent qu'elle réponde à un «* besoin social impérieux *» et, en particulier, qu'elle soit proportionnée au but légitime poursuivi et que les motifs invoqués par les autorités nationales pour la justifier apparaissent «* pertinents et suffisants *» (voir notamment,* M.K. c. France*, nº 19522/09, paragr. 33, 18 avril 2013).*

« 4. *S'il appartient tout d'abord aux autorités nationales de juger si toutes ces conditions se trouvent remplies, c'est à la Cour qu'il revient de trancher en définitive la question de la nécessité de l'ingérence au regard des exigences de la Convention (*Coster c. Royaume-Uni *[GC], nº 24876/94, paragr. 104, 18 janvier 2001, et* S. et Marper c. Royaume-Uni *[GC], nº 30562/04 et n° 30566/04, paragr. 101, CEDH 2008). Une certaine marge d'appréciation, dont l'ampleur varie et dépend d'un certain nombre d'éléments, notamment de la nature des activités en jeu et des buts des restrictions, est donc laissée en principe aux États dans ce cadre (voir notamment* Klass et autres c. Allemagne*, 6 septembre 1978, paragr. 49, série A nº 28,* Smith et Grady c. Royaume-Uni*, nº 33985/96 et n° 33986/96, paragr. 88, CEDH 1999-VI,* Gardel c. France*, nº 16428/05,* B. B. c. France*, nº 5335/06, et* M. B. c. France*, nº 22115/06, 17 décembre 2009, respectivement paragr. 60, 59 et 51). Cette marge est d'autant plus restreinte que le droit en cause est important pour garantir à l'individu la jouissance effective des droits fondamentaux ou d'ordre «* intime *» qui lui sont reconnus (*Connors c. Royaume-Uni*, nº 66746/01, paragr. 82, 27 mai 2004, et* S. et Marper*, précité, paragr. 102). En revanche, lorsqu'il n'y a pas de consensus au sein des États membres du Conseil de l'Europe, que ce soit sur l'importance relative de l'intérêt en jeu ou sur les meilleurs moyens de le protéger, la marge d'appréciation est plus large (*Dickson c. Royaume-Uni *[GC], nº 44362/04, paragr. 78, CEDH 2007-XIII).*

« 5. *La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. Cette nécessité se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Le droit interne doit notamment s'assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit aussi contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (*S. et Marper c. Royaume-Uni*, précité, paragr. 103,* Gardel c. France*, précité, paragr. 62, CEDH 2009, et* M. K. c. France*, précité, paragr. 35).*

« 6. *Pour apprécier le caractère proportionné de la durée de conservation des informations au regard du but poursuivi par leur mémorisation, la Cour tient compte de l'existence ou non d'un contrôle indépendant de la justification de leur maintien dans le système de traitement, exercé sur la base de critères précis tels que la gravité de l'infraction, les arrestations antérieures, la force des soupçons pesant sur la personne ou toute autre circonstance particulière (*S. et Marper c. Royaume-Uni*, précité, paragr. 119, et* B. B. c. France*, précité, paragr. 68).*

« 7. *Enfin, il appartient à la Cour d'être particulièrement attentive au risque de stigmatisation de personnes qui, à l'instar du requérant, n'ont été reconnues coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence. Si, de ce point de vue, la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donne pas l'impression de ne pas être considérés comme innocents (*S. et Marper*, précité, paragr. 122, et* M. K.*, précité, paragr. 36) ».*

ii. L'application des principes susmentionnés au cas d'espèce

« 8. *La Cour observe d'emblée que le requérant se plaint d'une atteinte susceptible d'être portée à sa vie privée et familiale du fait de son inscription au fichier, dans le cadre d'une éventuelle procédure devant le juge aux affaires familiales relative au droit de garde de son enfant. Or, elle constate que ce magistrat ne figure pas parmi les personnes ayant accès au fichier concerné. La situation dénoncée par le requérant n'est donc pas susceptible de se produire.*

« 9. *En revanche, s'agissant du caractère outrageant invoqué, la Cour note que si les informations répertoriées au STIC ne comportent ni les empreintes digitales (à la différence du fichier automatisé des empreintes digitales – voir* M. K.*, précité) ni le profil ADN des personnes, elles présentent néanmoins un caractère intrusif non négligeable, en ce qu'elles font apparaître des éléments détaillés d'identité et de personnalité en lien avec des infractions constatées, dans un fichier destiné à la recherche des infractions.*

« 10. *En outre, la Cour relève que le requérant a bénéficié, à la suite de la médiation pénale, d'un classement sans suite justifiant qu'il reçoive un traitement différent de celui réservé à une personne condamnée, afin d'éviter tout risque de stigmatisation (*S. et Marper*, précité, paragr. 22, et* M. K.*, précité, paragr. 42). À ce titre, elle observe que depuis la loi du 14 mars 2011, l'article 230-8 du code de procédure pénale dispose que, dans une telle hypothèse, le classement sans suite doit faire l'objet d'une mention sur la fiche enregistrée au STIC et les données relatives à la personne concernée ne peuvent alors plus être consultées dans le cadre de certaines enquêtes administratives. En l'espèce, la Cour ignore si la décision du ministère public a été effectivement inscrite parmi les informations concernant le requérant. Néanmoins, elle constate qu'en tout état de cause cette mesure n'a pas d'effet sur la durée de conservation de la fiche, qui est de vingt ans. Or, elle considère que cette durée est importante, compte tenu de l'absence*

de déclaration judiciaire de culpabilité et du classement sans suite de la procédure après le succès de la médiation pénale. Il lui appartient donc de s'interroger sur le caractère proportionné d'un tel délai, en tenant compte de la possibilité pour l'intéressé de demander l'effacement anticipé des données (voir mutatis mutandis*,* M. K.*, précité, paragr. 45).*

« 11. *À cet égard, la Cour relève que la loi, dans sa version applicable à l'époque des faits comme dans celle en vigueur, ne donne au procureur le pouvoir d'ordonner l'effacement d'une fiche que dans l'hypothèse d'un non-lieu ou d'un classement sans suite motivé par une insuffisance des charges, outre les cas de relaxe ou d'acquittement pour lesquels l'effacement est de principe mais où il peut prescrire le maintien des données au STIC. En l'espèce, pour rejeter la demande présentée à cette fin par le requérant, le procureur de la République d'Évry a appliqué strictement ces dispositions et s'est borné à constater que la procédure concernée avait fait l'objet d'une décision de classement sans suite, fondée sur une autre cause que l'absence d'infraction ou son caractère insuffisamment caractérisé. Il n'avait donc pas compétence pour vérifier la pertinence du maintien des informations concernées dans le STIC au regard de la finalité de ce fichier, ainsi que des éléments de fait et de personnalité. La Cour estime qu'un tel contrôle ne saurait passer pour effectif, l'autorité chargée de l'exercer n'ayant pas de marge d'appréciation pour évaluer l'opportunité de conserver les données.*

« 12. *De même, elle note qu'à l'époque des faits la décision du procureur de la République n'était susceptible d'aucun recours. Certes, d'une part, le droit interne permet désormais à l'intéressé d'adresser une nouvelle demande au magistrat référent visé à l'article 230-9 du code de procédure pénale, comme le soutient le Gouvernement. La Cour observe néanmoins que le texte précise que ce magistrat «* dispose des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles (...) que le procureur de la République *». Aux yeux de la Cour, un tel recours ne présente donc pas le caractère d'effectivité nécessaire, l'autorité décisionnaire ne disposant d'aucune marge d'appréciation quant à la pertinence du maintien des informations au fichier, notamment lorsque la procédure a été classée sans suite après une médiation pénale, comme en l'espèce. D'autre part, la jurisprudence récente du Conseil d'État reconnaît la possibilité d'exercer un recours pour excès de pouvoir contre les décisions du procureur en matière d'effacement ou de rectification, qui ont pour objet la tenue à jour du STIC et sont détachables d'une procédure judiciaire. Cependant, la Cour constate que cette faculté n'était pas reconnue à l'époque des faits, le requérant s'étant vu expressément notifier l'absence de toute voie de contestation ouverte contre la décision du procureur du 1er décembre 2009.*

« 13. *Ainsi, bien que la conservation des informations insérées dans le STIC soit limitée dans le temps, il en découle que le requérant n'a pas disposé d'une possibilité réelle de demander l'effacement des données le concernant et que, dans une hypothèse telle que celle de l'espèce, la durée de vingt ans prévue est en pratique assimilable, sinon à une conservation indéfinie, du moins à une norme plutôt qu'à un maximum (*M. K.*, précité).*

« 14. *En conclusion, la Cour estime que l'État défendeur a outrepassé sa marge d'appréciation en la matière, le régime de conservation des fiches dans le STIC, tel qu'il a été appliqué au requérant, ne traduisant pas un juste équilibre entre les intérêts publics et privés concurrents en jeu. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique.*

« 15. *Il y a donc eu violation de l'article 8 de la Convention. (...)*

« *Par ces motifs, la Cour, à l'unanimité,*

« 1. *Déclare la requête recevable quant aux griefs tirés de la violation des articles 8 et 13 et irrecevable pour le surplus ;*

« 2. *Dit qu'il y a eu violation de l'article 8 de la Convention* ».

2.3. Juridictions françaises

Conseil constitutionnel

C.C. décision n° 86-2010 DC du 29 juillet 1986, *Loi portant réforme du régime juridique de la presse*, § 20 à 24.

C.C. décision n° 86-217 DC du 18 septembre 1986, *Loi relative à la liberté de communication*, § 25 à 37.

C.C. décision n° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, §3.

C.C. décision n° 96-378 DC du 23 juillet 1996, *Loi de réglementation des télécommunications*, §28.

C.C. décision n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, §45.

C.C. décision n° 99-411 DC du 16 juin 1999, *Loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs*.

C.C. décision n° 2001-456 DC du 27 décembre 2001, § 45, *au sujet de la commission de vérification des fonds spéciaux.*

C.C. décision n° 2003-467 DC du 13 mars 2003, *Loi sur la sécurité intérieure*, §17 à 46.

C.C. décision n° 2004-496 du 10 juin 2004, *Loi pour la confiance dans l'économie numérique*, § 7 à 9.

C.C. décision n° 2004-499 DC du 29 juillet 2004, *Loi 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*, § 13.

C.C. décision n° 2005-532 du 19 janvier 2005, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*.

C.C. décision n° 2005-532 DC du 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.*

C.C. décision n° 2006-540 DC du 27 juillet 2006, *Loi relative au droit d'auteur et aux droits voisins dans la société de l'information*, § 15.

C.C. n° 2009-577 DC du 3 mars 2009, *Loi relative à la communication audiovisuelle et au nouveau service public de la télévision*, § 2.

C.C. décision n° 2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur Internet.*

C.C. décision n° 2010-25 QPC du 16 septembre 2010.

C.C. décision n° 2010-45 QPC du 6 octobre 2010.

C.C. décision n° 2011-625 DC du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*, §9 à 19.

C.C. décision n° 2011-192 QPC du 10 novembre 2011.

C.C. décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*, §8.

C.C. décision n° 2014-690 DC du 13 mars 2014, *Loi relative à la consommation*, § 57.

Conseil d'État

CE, Ass. 6 novembre 2002*, M. Moon et Mme Hak Ja Han M,* n° 194295, Rec. p. 380.

CE, 9 avril 2004, *M. X*, n° 263759 Conseil d'État, n° 263759.

CE, 11 avril 2014, *Ligue des droits de l'homme*, n° 360759.

CE 31 juillet 2009, *Association Aides et autres*, n° 320196, Rec. p. 341.

CE, Ass., 26 octobre 2011, *Association pour la promotion de l'image,* n° 317827, Rec. p. 505.

CE, 12 mars 2014, *Société Pages Jaunes groupe*, n° 353193.

> « *(...) En ce qui concerne le premier motif, tiré de la collecte déloyale des données et de l'absence d'information des personnes quant à l'indexation de leurs profils sur les réseaux sociaux :*
>
> « 9. *Considérant qu'il est constant que les membres des réseaux sociaux :* Copains d'avant*,* Facebook*,* Twitter*,* Trombi*,* Linkedin *et* Viadeo *n'ont été informés de l'extraction de leurs données à caractère personnel vers le service d'annuaire* Pages Blanches *ni au moment de l'enregistrement des données, ni lorsque celles-ci ont été communiquées pour la première fois à un tiers ; que la circonstance que, dans le cadre de leur politique de confidentialité, certains de ces réseaux sociaux auraient averti leurs membres de la possible indexation de ces données par des moteurs de recherche ne saurait faire regarder ceux-là comme déjà informés, au sens des dispositions précitées du III de l'article 32 de la loi du 6 janvier 1978, de la possible agrégation de leurs données à caractère personnel à un service d'annuaire ; qu'eu égard à l'intérêt qui s'attache au respect des libertés et droits fondamentaux des vingt-cinq millions de personnes touchées par le traitement litigieux, et notamment au respect de leur vie privée, la société* Pages Jaunes groupe *n'est pas fondée à soutenir que l'information de ces personnes, dont elle avait les coordonnées, exigeait des efforts disproportionnés par rapport à l'intérêt de la démarche au sens des dispositions précitées du III de l'article 32 ; qu'il*

suit de là que la formation restreinte de la CNIL n'a pas fait une inexacte application des dispositions du 1° de l'article 6 de la loi du 6 janvier 1978 en estimant que les données à caractère personnel extraites de réseaux sociaux en vue de leur mention dans le service d'annuaire Pages Blanches *n'ont pas été collectées de manière loyale et licite, faute de consentement explicite et éclairé des intéressés ; (...)*

« *En ce qui concerne le quatrième motif, tiré du non-respect des droits des personnes :*

« 13. *Considérant qu'aux termes de l'article 38 de la loi du 6 janvier 1978 : «* Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (...) *» ; qu'aux termes de l'article 40 de la même loi : «* Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite (...) *» ; que l'article 94 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 fait obligation au responsable du traitement, lorsque la demande formulée sur le fondement des articles 38 à 40 de cette loi est imprécise ou incomplète, d'inviter le demandeur à lui fournir, dans le délai de deux mois qui suit sa demande, les éléments lui permettant de procéder aux opérations qui lui sont demandées ;*

« 14. *Considérant qu'il résulte de l'instruction, en premier lieu, que les personnes dont les données à caractère personnel étaient extraites de réseaux sociaux pour être agrégées au service d'annuaire* Pages Blanches *n'étaient informées de leur droit d'opposition que si elles consultaient ce service ; qu'en deuxième lieu, le droit d'opposition ne pouvait pas être exercé de manière effective et durable, eu égard à la complexité de la procédure et à la circonstance que les demandes imprécises ou incomplètes n'étaient pas traitées ; qu'en troisième lieu, l'exercice du droit de rectification n'était pas garanti, le responsable du traitement estimant qu'il en était exonéré du fait du caractère indirect de la collecte des données ; qu'ainsi, la formation restreinte de la CNIL, qui est légalement tenue de garantir, sous le contrôle du juge, l'effectivité du droit d'accès, de rectification et d'opposition, n'a pas commis d'erreur de droit en estimant que la société* Pages Jaunes groupe *avait méconnu les dispositions des articles 38 et 40 de la loi du 6 janvier 1978 ;*

« *En ce qui concerne le cinquième et dernier motif, tiré du non-respect de l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données :*

« 15. *Considérant qu'il est constant que la société* Pages Jaunes groupe *collectait les adresses IP associées aux contenus, date et heure des requêtes effectuées sur son portail ; qu'elle justifie cette collecte de données par la nécessité de répondre aux demandes d'information des autorités administratives et judiciaires ; que, toutefois, une telle collecte porte atteinte*

aux droits fondamentaux des personnes ; que, ne répondant à aucune obligation légale, elle ne peut pas être regardée comme étant en relation directe avec l'objet même du traitement ; que, par suite, c'est à bon droit que la formation restreinte de la CNIL a considéré que cette collecte de données inadéquates méconnaissait les dispositions du 3° de l'article 6 de la loi du 6 janvier 1978 ;

« 16. *Considérant qu'il résulte de ce qui précède que la société* Pages Jaunes groupe *n'est pas fondée à demander l'annulation de l'avertissement qui lui a été infligé par la formation restreinte de la CNIL* ».

Cour de Cassation

Cass. Ass. Plen., 7 mars 1986, *Atari,* n°84-93509.

Cass. Com., 4 décembre 2001, n°99-16-642.

Cass. Crim., 9 septembre 2008, *Giuliano F.*, n°07-87.281.

Cass. Crim., 15 décembre 2010, n°10-83764.

Cass. Soc., 3 novembre 2011, n°10-18.036.

Cass. Com., 3 mai 2012, *eBay contre Société Parfums Christian Dior et autres*, n°11-10.508.

Cass. Civ. 1ère, 12 juillet 2012, *Auféminin.com et Google France.*

Cass. Com., 25 juin 2013, n° 12-17.037.

Tribunal de grande instance de Paris

TGI Paris, 3 novembre 1998, *UNADIF c/ Faurisson*.

TGI Paris, 26 février 2002, *Yahoo!.*

TGI Paris, 6 novembre 2013, *Max Mosley c/ Google Inc et Google France*, RG 11/07970.

« *Sur les demandes tendant à ce que soit interdit à la société* Google Inc *de référencer neuf images portant atteinte à la vie privée du demandeur :*
« *Attendu qu'ainsi que cela a été précédemment relevé, le tribunal est saisi d'une demande visant à interdire au responsable du moteur de recherche* Google images *de reproduire sur ses pages de résultats, neuf clichés photographiques provenant d'un enregistrement jugé attentatoire au respect dû à sa vie privée et constitutif d'une infraction pénale ;*

« *Attendu que la société* Google Inc *indique dans ses écritures que son service de référencement d'images, dénommé* Google images *«* fonctionne de la même façon que les moteurs de recherche traditionnels *», précisant que «* des programmes informatiques (robots) indexent constamment et de manière totalement automatique l'ensemble de l'Internet et recueillent l'information ainsi partagée volontairement par des millions d'éditeurs de sites, voire les auteurs de contenus eux-mêmes » ;

« *Qu'elle précise qu'en «* pratique, à la suite d'une requête effectuée sur le site http://images.google.fr/, le moteur Google Images fournit aux internautes

une liste de résultats, présenté sous forme de vignettes en basse résolution et dont la source a été identifiée par l'algorithme comme répondant aux mots-clés de l'internaute *», vignettes qui peuvent être grossies et qui sont dotées d'un lien hypertexte permettant d'accéder «* au site d'origine » ;

« *Attendu que la société* Google Inc *estime que les mesures sollicitées par le demandeur se heurtent à trois principes qui doivent guider les juridictions ayant à trancher un tel litige : la nécessité d'une base légale, la proportionnalité de la mesure au regard des droits fondamentaux que sont la liberté de communiquer des informations et la liberté d'entreprise et, enfin, la prohibition des arrêts de règlements ;*

« *Attendu que le caractère illicite de la diffusion des images provenant de cet enregistrement de scènes relevant de la sphère la plus intime de la vie privée, apparaît avec l'évidence qui a été constatée par le juge des référés de ce siège dans son ordonnance du 29 avril 2008, estimant que le fait que des atteintes du type de celle dont a été victime Max Mosley, soient pénalement réprimées était une «* marque de civilisation *» ; que ces images ont été jugées constitutives d'un délit pénal en France et sanctionnées par une juridiction britannique ; que le tribunal considère que la publication de ces images porte atteinte au droit de Max Mosley au respect de sa vie privée ;*

« *Attendu que, contrairement à ce qu'affirme la société défenderesse, le droit français prévoit, notamment dans l'article 9 du code civil, la possibilité pour les juges de «* prescrire toutes mesures, (…) propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée *», que ce texte, très général quant aux mesures qui peuvent être prises, inclut celles de nature à «* empêcher *» une telle atteinte et permet donc de prendre des mesures pour l'avenir avant que l'atteinte ne soit réalisée ;*

« *Qu'en outre, et à supposer que l'activité de moteur de recherche permette à la société défenderesse, comme elle le prétend, d'être rangée dans la catégorie des prestataires intermédiaires techniques, au sens de la directive 2000/31, cette qualité ne fait pas obstacle à ce que lui soient imposées des obligations de retrait ou d'interdiction d'accès dès lors que, ainsi que le prévoient les considérants 45, 46 et 47 de cette directive, il peut être imposé à ces prestataires de retirer des informations ou de rendre leur accès impossible ; qu'en application de cette directive, l'article 6-I-8° de la loi du 21 juin 2004 dite «* LCEN *», prévoit que l'autorité judiciaire peut prescrire à ces prestataires intermédiaires «* 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 *», y compris comme le prévoit le 7° «* des activités de surveillance ciblées et temporaires *»; que l'article L. 32-3-4 du code des postes et des communications électroniques prévoit également la possibilité pour les autorités judiciaires d'ordonner le retrait du réseau des contenus transmis initialement ou d'en rendre l'accès impossible ;*

« *Que la mesure sollicitée de retrait et d'interdiction pour l'avenir des neufs clichés photographiques provenant d'un délit pénal et déjà jugés*

attentatoires à la vie privée du demandeur, entre largement dans ce cadre légal, même si la société défenderesse pouvait être qualifiée de prestataire intermédiaire ;

« *Que sans doute, et comme le fait valoir à bon droit la société* Google Inc*, les mesures ordonnées doivent elles être proportionnées et limitées dans le temps ;*

« *Que, s'agissant du caractère proportionné de la demande visant au retrait et à l'interdiction de publication sur le moteur de recherche exploité par la demanderesse de neuf images issues de la vidéo litigieuse, il doit être relevé que cette condition est en l'occurrence parfaitement remplie au regard, d'une part, de l'obligation positive qui pèse sur la France en vertu l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, de faire respecter le droit subjectif de Max Mosley au respect de sa vie privée et, d'autre part, de l'impossibilité où se trouve le demandeur de faire respecter ce droit en n'usant que des seules procédures mises à sa disposition par la défenderesse, soit une demande réitérée à chaque nouvelle mise en ligne d'une de ces images avec l'indication de son URL, procédures qu'il a suivies pendant près de deux ans en vain, ces images, compte tenu de leur nature, réapparaissant sur les pages de résultats du moteur de recherche de la société* Google Inc *systématiquement après une suppression ; qu'ainsi, il est établi que les exigences de la société* Google Inc *sont inappropriées en l'espèce pour que le droit de Max Mosley soit respecté ; que la mesure sollicitée tendant à obtenir que neuf des images issues de la vidéo en cause n'apparaissent pas sous forme de vignette comme résultat du moteur de recherche est de nature, sinon à supprimer les atteintes portées, du moins à en réduire sensiblement leur portée ;*

« *Que la mesure sollicitée poursuit ainsi un but légitime, la société* Google Inc *ne démontrant nullement que la diffusion de ces images serait légitime, se bornant à soutenir à cet égard qu'elle «* ne peut tolérer d'être instrumentalisée *» pour prendre en charge la réputation de Max Mosley sur Internet, alors que la mesure de retrait et d'interdiction de référencement par la société* Google Inc *de ces images tend à éviter que ce moteur de recherche, en publiant ces images illicites sur les pages de résultats ne participe, en les amplifiant, aux incontestables atteintes qui sont portées sur divers sites Internet, au respect dû à sa vie privée ;*

« *Que cette mesure est également «* nécessaire dans une société démocratique *» au sens de l'article 10 paragr. 2 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, l'illicéité de ces images étant manifeste et ayant été judiciairement constatée par des juridictions de deux États européens ; qu'il doit être observé que l'interdiction de publier ces images sur les pages de résultats du moteur de recherche* Google images *ne fait naturellement pas obstacle à ce que cette «* affaire judiciaire au retentissement international *», comme la qualifie la demanderesse, fasse l'objet de commentaires référencés sur le moteur de recherche, les demandes ne portant que sur la reproduction d'images ;*

« *Attendu, en revanche, que la contestation par la société* Google Inc *de l'absence de limite dans le temps de la mesure sollicitée qui la rend trop absolue, doit être admise ; (…)*

« *Attendu enfin, que la société défenderesse fait valoir que le tribunal ne pourrait réparer et ordonner des mesures d'interdiction visant d'autres sites que* google.fr*, qui ne visent pas le public de France en application des principes régissant les règles de compétence en cette matière et également compte tenu du fait que de nombreux sites référencés par* Google images *sont des sites rédigés en langue étrangère ;*

« *Attendu cependant – et abstraction faite de la contradiction qui affecte la position de la défenderesse qui affirme que son moteur de recherche est totalement neutre et passif et soutient que les pages de résultats figurant sur les divers sites Internet qu'elle exploite dans le monde pourraient être différentes – que le présent litige porte sur le référencement effectué grâce au moteur de recherche* Google images *que la société* Google Inc *dit être seule à exploiter et à en avoir la maîtrise ; que, s'agissant d'images, il appartient à la société défenderesse de démontrer que les référencements sur des sites Internet qu'elle exploite et qu'elle dit être destinés à un autre public que celui situé sur le territoire français, n'ont pas d'impact sur ce territoire où ces images ont été jugées constitutives d'une infraction pénale ;*

« *Attendu, en conséquence, qu'il sera fait injonction, sous astreinte dans les conditions précisées dans le dispositif, à la société* Google Inc *de retirer et de cesser l'affichage sur le moteur de recherche* Google images *qu'elle exploite, accessible en France, des neuf images figurant aux pages 16 et 17 des conclusions de Max Mosley régulièrement signifiées par voie électronique le 5 novembre 2012, pendant une durée de cinq ans à compter de l'expiration du délai de deux mois suivant la signification de la présente décision ; (…) ».*

2.4. Autorités administratives indépendantes

Autorité de la concurrence

Autorité de la concurrence, décision n° 10-MC-01 du 30 juin 2010, *relative à la demande de mesures conservatoires présentée par la société Navx (affaire Navx c/ Google).*

Autorité de la concurrence décision n° 10-D-30 du 28 octobre 2010*, relative à des pratiques mises en œuvre dans le secteur de la publicité sur Internet.*

Autorité de la concurrence avis n° 10-A-29 du 14 décembre 2010, *sur le fonctionnement concurrentiel de la publicité en ligne.*

Autorité de la concurrence, avis n° 11-A-10 du 29 juin 2011, *portant sur la mise en place d'un tarif social permettant l'accès des personnes aux revenus modestes aux services Internet haut débit.*

Autorité de la concurrence, décision n° 12-D-18 du 20 septembre 2012, *relative à des pratiques mises en œuvre dans le secteur des prestations d'interconnexion réciproques en matière de connectivité Internet.*

CNIL

CNIL, délibération n° 2006-066 du 16 mars 2006.

CNIL, délibération n° 2010-096 du 8 avril 2010.

CNIL, communication n° 12-17.037 du 25 juin 2013.

CNIL, délibération n° 2013-420 du 3 janvier 2014.





Annexe 3 : La notion d'autodétermination informationnelle (« Informationnelle Selbstbestimmung »)

(source : Conseil d'État, centre de recherches et de diffusion juridiques, cellule de droit comparé).

1. Les contours de la notion

Cette notion recouvre, en Allemagne, un droit constitutionnel d'origine prétorienne né de l'interprétation combinée des articles 1 et 2 de la Loi fondamentale par la Cour constitutionnelle fédérale (« *Bundsverfassungsgericht* »). L'article 2 porte sur les droits de la personne et affirme le droit de chacun au libre épanouissement de sa personnalité, l'article 1 proclame l'intangibilité de la dignité humaine. La finalité originelle de ce droit était de permettre à l'individu de se défendre contre les atteintes pouvant être portées, par l'État, à sa liberté individuelle, mais il a, par la suite, été également invoqué dans des litiges entre particuliers, notamment en droit du travail.

L'autodétermination informationnelle, telle que définie par l'arrêt de principe *Volkszählungsgesetz*[208] (en français, loi sur le recensement) de la Cour constitutionnelle fédérale (BVerfGE 65, 1 du 15 décembre 1983) implique le droit pour chacun de contrôler la divulgation et l'utilisation de ses données personnelles et, en conséquence, celui de décider quand et à l'intérieur de quelles limites les circonstances de sa vie personnelle peuvent être rendues publiques (arrêt *Volkzählungsgesetz*). Le droit à l'autodétermination informationnelle est vu en doctrine comme une branche spécialisée du droit général de la personnalité.

De la consécration de ce droit comme un droit fondamental découlent les conséquences suivantes :

- Toute restriction à son libre exercice doit être justifiée par un intérêt public essentiel (« *überwiegend* »), la restriction doit être absolument nécessaire. L'article 1er de la Loi fondamentale ancre l'individu, dont les droits fondamentaux doivent être respectés, dans la communauté humaine et permet de ce fait de porter atteinte à ces droits lorsque la protection de la communauté le requiert.

208 Cet arrêt a été rendu à propos d'une loi de 1983 mettant en place un recensement et prévoyant le traitement informatisé des données ainsi recueillies. La publication des questions devant être posées dans le cadre du recensement a donné lieu à un nombre important de plaintes constitutionnelles individuelles (« *Verfassungsbeschwerde* ») et à des appels au boycott du recensement. Les critiques visaient tout particulièrement la comparaison prévue entre les données recueillies et les données existantes issues des registres communaux (en Allemagne toute installation dans une commune s'accompagne d'une obligation de s'enregistrer). Étaient également mis en cause le nombre des questions posées et leur caractère détaillé susceptibles, d'après les critiques, de permettre l'identification des personnes interrogées. La Cour ayant déclaré inconstitutionnelles certaines dispositions de la loi, le référendum prévu a été annulé et n'a été réalisé qu'en 1987.

- Le danger ne doit pas être hypothétique mais concret (« *konkret* »), imminent (« *drohende Gefahr* »). Tout danger pour la sécurité publique ne justifie pas une atteinte au droit à l'autodétermination informationnelle. Il doit s'agir d'une menace importante (« *erheblich* ») pour l'intégrité physique, la vie ou la liberté des personnes ou encore la sécurité de l'État fédéral ou celle des *Länder*.

- Les restrictions au libre exercice du droit à l'autodétermination informationnelle doivent être fondées sur une loi qui réponde à l'exigence constitutionnelle de clarté de la norme (« *Normenklarheit* »). Le législateur doit réglementer tant le contenu de la mesure attentatoire que la procédure gouvernant sa mise en œuvre. Les dispositions portant atteinte au droit fondamental doivent être précises (« *Bestimmtheit* »*).*

- Le moyen utilisé pour parvenir à l'objectif de protection de l'intérêt public doit être le moins attentatoire possible aux libertés de la personne. L'atteinte portée doit être proportionnée au but d'intérêt général poursuivi. Plus la mesure est susceptible de porter atteinte au cœur des droits de la personne[209], plus l'intérêt public qui la légitime doit être important. Enfin, la gravité de l'atteinte s'apprécie également au regard du risque d'utilisation ultérieure des données collectées, ainsi que de la durée prévue pour leur conservation.

2. Application par les juridictions

La Cour constitutionnelle fédérale (« *Bundesverfassungsgericht – BVerfG* ») et la Cour administrative fédérale (« *Bundesverwaltungsgericht – BverwG* ») ont rendu plusieurs arrêts qui ont permis de dégager les contours de la notion d'autodétermination informationnelle.

2.1. Condition tenant à l'existence d'un but légitime

Fiscalité
Décision du 27 juin 1991, BVerfG 84, 239 *Zinsenbesteuerung* :
La Cour constitutionnelle fédérale a considéré que le recueil de données portant sur les intérêts perçus sur le capital est compatible avec le respect de l'autodétermination informationnelle, car il est indispensable à l'établissement de l'impôt et au respect du principe d'égalité devant ce dernier.

Prévention de la criminalité et des actes terroristes
L'installation dans un lieu public de caméras vidéo capables de fournir des images en gros plan de plan de personnes permettant leur identification et une vision détaillée de leurs activités est *a priori* contraire à leur droit à l'autodétermination

209 « Der Kernbereich privater Lebensgestaltung » : le noyau intangible de la sphère privée d'une personne, BVerfG, 9. 11. 2010 – 2 BvR 2101/09, c'est-à-dire son intimité, notamment ses orientations religieuses ou sexuelles.

informationnelle nonobstant l'apposition de pancartes informant le public de ce fait. Toutefois la prévention de la criminalité constitue un intérêt public de rang supérieur et prévaut donc sur la nécessaire préservation des droits de la personnalité.

Décision du 25.01.2012*, BVerwG Reeperbahn* :
La Ville de Hambourg avait installé des caméras vidéo sur le *Reeperbahn*, l'artère traversant un quartier caractérisé par une importante activité de prostitution. La requérante, habitante du quartier se plaignait d'une atteinte à son droit à l'autodétermination informationnelle car la caméra, installée à proximité de son logement, était équipée d'un cache empêchant de filmer les appartements mais enregistrait les va-et-vient se produisant dans le hall d'entrée. La Cour administrative fédérale a considéré que l'atteinte n'était pas démesurée s'agissant d'une zone à haut taux de délinquance et a souligné que la requérante bénéficiait elle-même de la protection offerte par les caméras.

Décision du 13 juin 2007, *Rasterfahndung, BVerfG* 115, 320 :
La prévention du terrorisme peut justifier une atteinte continue (« *dauerhaft* »*)* au droit à l'autodétermination informationnelle. Les dommages susceptibles de résulter d'actes de terrorisme peuvent, en effet, se matérialiser à tout moment. La mesure attentatoire aux droits de la personne ne pourra, toutefois, être mise en œuvre que s'il existe des éléments matériels permettant de conclure à la probabilité d'une attaque. Une menace générale telle que seule résultant des événements du 11 septembre ne suffit pas à légitimer une mesure préventive de *profilage* par recoupement de données (« *Rasterfahndung* »*)*.

2.2. Condition tenant à la proportionnalité de l'atteinte

L'exigence de proportionnalité est respectée, lorsque la surveillance vidéo se limite à des lieux où la délinquance est importante (« *Reeperbahn* »).

Décision du 11 août 2009, *BVerfG*, *2 BvR 941/08* :
Les preuves de délits routiers obtenues par le biais de caméras enregistrant le trafic ont été jugées inexploitables. En effet, dans la mesure où le numéro d'immatriculation et le conducteur du véhicule étaient parfaitement identifiables, elles portaient atteinte au droit à l'autodétermination informationnelle, alors même que l'administration ne disposait d'aucun élément concret permettant de soupçonner la commission de délits aux endroits où les caméras étaient installées.

Décision du 13 juin 2007*, Rasterfahndung, BVerfG 115, 320*,
Décision du 24 avril 2013, *Antiterrordatei BVerfG 1 BvR 1215/07* :
L'établissement de *profils* en croisant des données issues de plusieurs sources, ou le recours à des moyens de surveillance permettant une observation rapprochée, constituent des atteintes massives au droit à l'autodétermination informationnelle et ne peuvent, donc, être justifiés que par la protection d'un intérêt particulièrement important en présence d'une menace concrète et imminente.

2.3. Condition tenant à la base juridique

Il ne peut être porté atteinte au droit à l'autodétermination informationnelle sur la base d'une circulaire administrative (*BVerfG, 2 BvR 941/08*).

Le fondement légal de la mesure doit faire apparaître les éléments de faits prouvant le caractère concret de la menace.

Le recueil des informations doit poursuivre le but qui lui a été assigné par le législateur, et qui doit être défini avec précision dans la loi (Décision du 24 janvier 2012, *Kontostammdaten BVerfG*, 118,168).

Annexe 4 : Bibliographie indicative

1. Ouvrages

Babinet G., *L'ère numérique, un nouvel âge de l'humanité : Cinq mutations qui vont bouleverser notre vie*, Le Passeur, 2014.

Bellanger P., *La souveraineté numérique*, Stock, 2014.

Bensoussan A., *Code informatique, fichiers et libertés,* Larcier, 2014.

Bryjnolfsson E. McAfee A., *The Second Machine Age. Work, Progress and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company, New York, 2014.

Casilli A., Sarabi Y., Tubaro P., *Against the Hyposthesis of the End of Privacy,* Springer, 2014.

Colin N., Verdier H., *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2012

Frayssinet J., *Informatique, fichiers et libertés*, éd., Litec, Paris, 1992.

Frayssinet J., *L'Internet et la protection juridique des données personnelles. L'Internet et le droit* ? éd ; Victoires, 2001.

Hildebrandt M., Rouvroy A. (dir.), *Law, Human Agency and Autonomic Computing. The Philosophy of Law meets the Philosophy of Technology,* Routledge, 2011.

Huet J., Maisl H., *Droit de l'informatique et des télécommunications*, Litec, 1989.

Jarvis J., *Public parts: How sharing in the digital age improves the way we work and live. New York*, Simon & Schuster, 2011.

Laffaire M.-L., *Protection des données à caractère personnel*, éd. d'organisations, 2005.

Lepage A., *Libertés et droits fondamentaux à l'épreuve de l'Internet*, Litec, *Juris-Classeur*, 2002.

Lucas A., Deveze J., J. Frayssinet J., *Droit de l'informatique et de l'Internet*, PUF, 2001.

Mayer-Schönberger V., Cukier K., *Big Data. La révolution des données est en marche*, Robert Laffont, 2014.

Nissenbaum H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Stanford University Press, 2010.

Rahal-Löfskog D., Morlet-Haïdara L. (dir.), *La télémédecine et la protection des données de santé par la loi «informatique et libertés»,* Revue générale de droit médical n°42, 2012.

Rey B., *La vie privée à l'ère du numérique*, Lavoisier, 2012.

Schmidt E., Cohen J., *The New Digital Age, Reshaping the Future of People, Nations and Business*, Knopf, 2013.

Sillard B., *Maîtres ou esclaves du numérique?,* Éditions Eyrolles, 2011.

Sonnac N., Gabszewicz J., *L'Industrie des médias à l'ère numérique*, La Découverte, 3ème éd., 2013.

Strowel A., *Quand Google défie le droit*, De Boeck-Larcier, 2011.

2. Rapports

Alvergnat C., *Le publipostage électronique et la protection des données personnelles, Rapport adopté par la CNIL*, le 14 octobre 1999.

ANSSI, *Maîtriser la SSI pour les systèmes industriels*, janvier 2014.

ARCEP, Neutralité *de l'Internet et des réseaux. Propositions et recommandations*, septembre 2010.

Batho D., Bénisti J.-A., *Les fichiers de police*, rapport d'information de la commission des lois de l'Assemblée nationale, mars 2009.

Braibant G., *Données personnelles et société de l'information*. Rapport au Premier ministre sur la transposition de la directive n° 95/46, p. 32, mars 1998.

Bras P.-L., Loth A., *Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013.

CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur*, juin 2013.

CNIL, *Conclusions du contrôle du système de traitement des infractions constatées (STIC)*, janvier 2009.

Collin P. et Colin N., *Mission d'expertise sur la fiscalité de l'économie numérique*, rapport au ministre de l'économie et des finances, au ministre du redressement productif, au ministre délégué chargé du budget et à la ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, janvier 2013.

Commission européenne, Livre vert sur *La convergence des secteurs des télécommunications, des médias et des technologies de l'information, et les implications pour la réglementation*, COM (97)623, décembre 1997.

Conseil d'État, *Internet et les réseaux numériques*, La Documentation Française, 1998.

Conseil national du numérique, *Citoyens d'une société numérique*, novembre 2013.

Conseil national du numérique, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014.

CSA, *Rapport au Gouvernement* sur *l'application du décret n° 2010-1379 du 12 novembre 2010*, novembre 2013.

Council on Foreign Relations, Independent Task Force, *Defending an Open, Global, Secure and Resilient Internet,* Report n° 70, 2013.

Erhel C.,et De la Raudière L., *Rapport d'information sur la neutralité de l'Internet et des réseaux,* commission des affaires économiques de l'Assemblée nationale, avril 2011.

Europol, *EU Terrorism Situation and Trend Report*, 2013.

FING, *Nouvelles approches de la confiance numérique*, février 2011.

Gorce G., F. Pillet F., *Mission d'information du Sénat sur l'open data et la vie privée*, avril 2014.

IGF, *Le soutien à l'économie numérique et à l'innovation*, janvier 2012.

Imbert-Quaretta M., *Rapport sur les moyens de lutte contre le* streaming *et le téléchargement direct illicites*, février 2013.

Imbert-Quaretta M., *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne*, mai 2014.

La Rue F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Nations Unies, mai 2011.

Lemoine P., *La Transformation numérique de l'économie*, *rapport au ministre de l'économie et des finances, au ministre de la Décentralisation et de la fonction publique, au secrétaire d'État à la Réforme de l'État*, novembre 2014.

Lescure P., *Culture – acte 2. Contribution aux politiques culturelles à l'ère numérique*, mai 2013.

Livre blanc sur la « Défense et sécurité nationale », La Documentation française, avril 2013.

Livre blanc sur La France : Défense et sécurité nationale, Paris, Odile Jacob/La Documentation, juin 2008.

McKinsey Global Institute, *Big Data: The next frontier for innovation, competition and productivity*, mai 2011.

Morin-Desailly C., *L'Union européenne, colonie du monde numérique ?,* Rapport fait au nom de la commission des affaires européennes du Sénat, mars 2013.

OCDE, *Measuring the Internet Economy: A Contribution to the Research Agenda*, **OECD Digital Economy Papers**, n° 226, OECD Publishing, 2013.

Paul C., *Du droit et des libertés sur l'Internet*, La Documentation française, 2000.

President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World, Report and Recommendations*, décembre 2013.

Truche P., Faugère J.-P., Flichy P., *Administration électronique et protection des données personnelles*, Livre blanc, février 2002.

Urvoas J.-J et Verchère P., *Mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, Assemblée nationale, mai 2013.

Urvoas J.-J., P. Verchère P., *Rapport d'information de la commission des lois déposé en application de l'article 145 du règlement, par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, mai 2013.

World Economic Forum, *Unlocking the Value of Personal Data : from Collection to Usage*, février 2013.

3. Articles

Ballet P., « Où en est la procédure d'agrément des hébergeurs de données de santé à caractère personnel ? », *Gazette du Palais*, 18-19 avril 2007, p. 20.

Barbry E., Leperlier V., « Le transfert des données passagers vers les États-Unis face à l'impératif de protection des données personnelles », *Gazette du Palais*, 2004, 1, p. 88.

Barbry E., « Le droit du commerce électronique, de la protection à la confiance », *Droit Informatique et télécoms*, 1998.

Barnes S., « A privacy paradox: Social networking in the United States», First Monday, Vol. 11, n° 9, septembre 2006.

Basilien-Gainche M.-L., « Une prohibition européenne claire de la surveillance électronique de masse », *in Revue des droits de l'homme*, 14 mai 2014, [En ligne], Actualités Droits-Libertés, URL : http://revdh.revues.org/746.

Belloir P., « Le délit de collecte déloyale de données à caractère personnel à l'épreuve d'Internet », *Revue Lamy Droit de l'Immatériel*, 2006, n° 17.

Bensoussan A., « Le Correspondant à la protection des données à caractère personnel : un maillon important de la réforme », *Gazette du Palais*, 2004, 2, p. 3013.

Bern T., Rouvroy A., « Gouvernementalité algorithmique et perspectives d'émancipation » Réseaux, 2013/1.

Busseuil G., « Arrêt Google : du droit à l'oubli de la neutralité du moteur de recherche », *JCP E*, 2014, 1327.

Cauvin E., « Quelles lois pour le numérique ? », *Le Débat* 1/ 2011, n° 163, p. 16.

CNIL, « Le corps, nouvel objet connecté », *Cahiers Innovation et Prospective*, n° 2, mai 2014.

CNIL, « Le quantified self : nouvelle forme de partage des données personnelles, nouveaux enjeux ? », *La lettre Innovation & Prospective*, n° 5, juillet 2013.

Coslin C., Maxwell W., « L'efficacité à l'étranger des décisions françaises en matière de communication : le cas des États-Unis et du Premier Amendement », *Légicom*, n° 52, 2014.

Cruysmans E., Strowel A., « Un droit à l'oubli face aux moteurs de recherche : droit applicable et responsabilité pour le référencement de données 'inadéquates, non pertinentes ou excessives' », *Journal des tribunaux*, vol. 24, n° 6568, p. 457 – 459, juin 2014.

Debet A., « Internet et vie privée. La protection et la liberté du mineur internaute », *Communication Commerce électronique*, Décembre 2005, n° 12, étude 40.

Delaunay B., « Liberté d'accès aux documents administratifs et réutilisation des informations publiques, *AJDA*, 2006, p. 1377.

Drouard E., Hurel C., « Les fichiers de police », *Gazette du Palais*, 2006, 2, p. 2947.

Drouard E., Goussu G., Boccara V., « Loi «informatique et libertés». Des sanctions fortes, des risques accrus », *Petites affiches*, 16 février 2005, p. 3.

Falque-Pierrotin I., « La Constitution et l'Internet », *Nouveaux Cahiers du Conseil constitutionnel*, juin 2012, n° 36, p. 31.

Fauran B., « Loi «informatique et libertés» et données de recherche dans le domaine de la santé », *Gazette du Palais*, 2006, 1, p. 1698.

Fenoll-Trousseau M.-P., « Les moteurs de recherche, un piège pour les données à caractère personnel », *Communication Commerce électronique*, étude 3, 2006.

Forest D., « Pouvoirs de sanction de la CNIL : le réveil soudain d'une belle endormie », *D.*, 2007, p. 94.

Frayssinet J., « La régulation de la protection des données personnelles », *Legicom*, n° 42, 2009-1.

Frayssinet J., « Loi «informatique et libertés» et durée de conservation des données personnelles », *Revue Lamy droit de l'immatériel*, juin 2007, n° 916.

Gaudemet G., Perray R., « Le renforcement du rôle de la CNIL depuis 2004 », in *Regards sur l'actualité,* Documentation française, n° 327, janvier 2007, p. 71.

Gaudemet G., Perray R., « «*Scoring*» et protection des données personnelles. Un nouveau régime à l'efficacité incertaine », *Petites affiches*, 30 mai 2006, p. 8.

Gruber A., « Le système français de protection des données personnelles », *Petites affiches*, 4 mai 2007, p. 4.

Jacqué J.-P., « Protection des données personnelles, Internet et conflits entre droits fondamentaux devant la Cour de justice », *RTDE*, 2014, p. 283.

Latour X., « Le droit communautaire et la protection des données à caractère personnel dans le commerce électronique », *Petites affiches*, 6 février 2004 n° 27, p. 9.

Leclercq P., « La loi du 6 août 2004. Les transferts internationaux de données personnelles », *Communication Commerce électronique*, 2005, étude 8.

Ledieu M.-A., « Les fichiers des entreprises après la réforme du 6 août 2004 de la loi «informatique et libertés» », *Communication Commerce électronique*, 2004, étude 33.

Lepage A., « Censure par le Conseil constitutionnel d'une des dispositions de la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », *Communication Commerce électronique*, 2004, comm. 11.

Lepage A., « Les droits de la personnalité confrontés à l'Internet » *in Libertés et droits fondamentaux*, R. Cabrillac, M.-A. Frison-Roche, Th. Revet (ss dir.), Dalloz, 2007, p. 229.

Maitrot de la Motte A., « La réforme de la loi «informatique et libertés» et le droit au respect de la vie privée », *AJDA*, 2004, p. 2269.

Maxwell W., « La protection des données à caractère personnel aux États-Unis : convergences et divergences avec l'approche européenne », in *Le* cloudcomputing, Société de législation comparée, collection colloques, v.22, 2014.

Meisse E., « Directive n° 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 », *Europe*, 2002, comm. 324.

Milano L., « Un «droit à l'oubli» numérique consacré par la CJUE », *JCP G*, 2014, 1300.

Poullet Y. et Rouvroy A., « 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*, Benyekhlef K. & Trudel P. (dir.), Montréal, Thémis, 2009.

Poullet Y., « La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ? », *Legicom*, 2009/1.

Richard J. et Cytermann L., « Numérique/ il faut repenser la protection des droits fondamentaux », *AJDA*, 2014, p. 1684.

Robaczewski C., « Le droit à l'oubli », *Droit et Patrimoine*, 2014, p. 56.

Rosen J., "The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google", *80 Fordham L. Rev. 1525*, 2012.

Rosen, J., "The right to be forgotten", *64 Stan.L. Rev. Online 88.*

Rouvroy A., «Pour une défense de l'éprouvante inopérationnalité du droit face à l'opérationnalité sans épreuve du comportementalisme numérique.» *Dissensus. Revue de Philosophie Politique de l'Université de Liège,* n° 4, 2011.

de Saint Pulgent M. et Richard J., « Numérique : les rapports de droit sont des rapports de force », *AJDA*, 2014 p. 1625.

Schoettl J.-E., « La refonte de la loi sur l'informatique, les fichiers et les libertés devant le Conseil constitutionnel », *Petites affiches*, 11 août 2004, p. 8.

Senac C.-E., « Le droit à l'oubli en droit public », *RDP*, 2012, n° 4, p. 1156.

Simon D., « La révolution numérique du juge de l'Union – les premiers pas de la cybercitoyenneté », *Revue Europe*, vol. 24, n° 7, 2014, p. 4.

Treguer F., « Internet dans la jurisprudence de la Cour européenne des droits de l'homme », *Revue des droits et libertés fondamentaux*, mai 2013.

Wu T., « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003.

Comité de rédaction

Responsable de la publication :
Maryvonne de Saint Pulgent, présidente de la section du rapport et des études (SRE)

Conception et réalisation :
Maryvonne de Saint Pulgent, présidente de la SRE,
Corinne Mathey, secrétaire de la SRE

Secrétaire de rédaction :
Frédéric Navas Alonso de Castaneda, chargé de mission à la SRE,
avec la participation de Céline Bévillon, Morgane Bunel et Etienne Sèche, stagiaires à la SRE

Coordination du colloque

Jacky Richard, conseiller d'État, rapporteur général de l'étude annuelle 2014 du Conseil d'État « Le numérique et les droits fondamentaux »,
Marie Delord, secrétaire adjointe de la SRE

Crédits photos, conseil graphique : direction de la communication.