DOSSIER DU PARTICIPANT

Colloque du 6 février 2015

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

Un colloque organisé par le Conseil d'État

CONSEIL D'ÉTAT

I. PROGRAMME

9 h – 9 h 15 - Séance d'ouverture

- **Jean-Marc SAUVÉ,** vice-président du Conseil d'État

9 h 15 - 11 h - 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-LOFSKOG,** chef du service de la santé à la CNIL

11h – 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

12h45 – 14h Déjeuner libre

14 h – 15 h 45 - Table ronde n°3 : Le droit des Etats 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

- **Edouard 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

16h45 – 16 h 30 - 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

SEANCE D'OUVERTURE

Jean-Marc SAUVÉ

Vice-président du Conseil d'État

Diplômé de l'Institut d'études politiques (IEP) de 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.

TABLE RONDE 1 : QUELLE PROTECTION DES DONNEES PERSONNELLES POUR QUELLE CONCEPTION DE LA VIE PRIVEE ?

Problématique

La table ronde a pour ambition d'aborder la question sensible du statut des données personnelles. Y a-t-il un droit de propriété des personnes sur leurs données personnelles ? Ne convient-il pas plutôt d'envisager la protection des données personnelles comme un droit 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.

Intervenants

Président

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 le droit à l'oubli numérique, les droits de l'homme numérique, le droit des robots. C'est ainsi qu'il crée en 2014 l'Association du droit des robots. Président et fondateur de Lexing®, premier réseau international d'avocats dédié au droit des technologies avancées, il est également membre fondateur de l'Association française de droit de l'informatique et de la télécommunication, qu'il préside à deux reprises, membre fondateur et vice-président d'honneur de l'Association française des correspondants à la protection des données à caractère personnel, et, au sein de l'Union Internationale des Avocats, membre fondateur en 2006 de la Commission Droits de l'homme numérique, qu'il préside jusqu'en 2012. Il dispense un cours en droit de l'informatique à l'Ecole Centrale de Paris, est chroniqueur régulier dans différents médias et anime de nombreuses conférences et programmes de formation. Il a rédigé et publié de nombreux articles et ouvrages dont le plus récent, *Code Informatique, fichiers et libertés* est paru en octobre 2014.

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 (Ecole des Hautes Etudes 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 *Against the Hypothesis of the End of Privacy* (Springer, 2014). Ses ouvrages précédents incluent *Les liaisons numériques* (Seuil, 2010), une étude sur la façon dont le Web reconfigure les formes de la sociabilité contemporaine, et *Stop Mobbing* (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 la direction de l'institut de droit public et de science administrative en 2006. Il a également été professeur invité à la *Fletcher School of Law and Diplomacy* (2000), à l'université de Paris I 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 VIII^{ème} chambre du 7 octobre 2008 au 6 octobre 2009. Depuis le 11 octobre 2012, il est le président de la V^{ème} chambre.

Délia RAHAL-LOFSKOG

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 droit de la santé (université de Paris Sud), d'un DEA de l'École des hautes études en sciences sociales (La personne dans le droit), 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.

TABLE RONDE 2 : QUELLE REGULATION DES PLATEFORMES NUMERIQUES ?

Problématique

Le Conseil d'État propose la création d'une nouvelle catégorie juridique de « prestataires intermédiaires » 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 …), 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.

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…). Il organisa 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 ces 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'Ecole 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 en 2012-2013, après avoir fondé et présidé 1x1connect, société d'édition logicielle spécialisée dans le *social marketing*. Il est également fondateur de Stand Alone Media, société de production et d'édition vidéo à vocation encyclopédique. 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 par ailleurs l'auteur, avec Henri Verdier, de *L'Âge de la multitude, Entreprendre et gouverner après la révolution numérique* (Armand Colin, 2012) 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 membre du comité de direction de l'Institut Droit & Croissance et membre du groupe d'experts placé auprès de Philippe Lemoine dans le cadre de la mission sur la transformation numérique de l'économie nationale que lui a confiée le Gouvernement. 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'Etat 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 corédigé l'étude 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.

TABLE RONDE 3 : LE DROIT DES ETATS DANS UN UNIVERS TRANSNATIONAL : QUELLE TERRITORIALITE ?

Problématique

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. 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 du site internet.

La table ronde devra vérifier si la préconisation du Conseil d'Etat 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.

Intervenants

Président

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 œuvrant à l'harmonisation du droit des contrats ; elle participe actuellement à un groupe de travail de la Conférence de La Haye en vue de l'élaboration de principes sur la loi applicable aux contrats internationaux. Elle est par ailleurs directrice scientifique du Recueil Dalloz.

Intervenants

Édouard GEFFRAY

Secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL)

Edouard Geffray, maître des requêtes au Conseil d'Etat, 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'Etat 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, Edouard 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, Me 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, Me 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 200 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, avec C. Doutrelepont et Fr. Dubuisson), *Le téléchargement d'œuvres sur Internet* (Larcier 2012), *Net Neutrality in Europe - La neutralité de l'Internet en Europe*, (Bruylant, 2013, avec. A. Autenne et V. Cassiers), *Droit, Economie, Valeurs*, (Larcier, 2014).

CLOTURE - CONCLUSION A DEUX VOIX

Maryvonne de SAINT PULGENT

Présidente de la section du rapport et des études du Conseil d'État

Diplômée de l'Institut d'études politiques de 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 8ème 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 le titre de *privat-docent* en 2006 et le titre de docteur en droit en 2000 à l'université de Münich. En 2014, il a enseigné les relations entre divers systèmes de droit à l'université Panthéon-Assas à Paris 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).

I. ANALYSE DES MESURES PROPOSEES DANS L'ETUDE ANNUELLE 2014

La liste exhaustive des 50 propositions est donnée en partie V.

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'« *empowerment* », « d'autonomisation » des individus, 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, ainsi 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. Définir les principes fondant la protection des droits fondamentaux à l'ère du numérique

Il est parfois proposé de reconnaître aux individus un véritable droit de propriété sur leurs données, en pariant sur leur plus grande implication du fait qu'ils deviendraient financièrement intéressés 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 celui-ci comme un **droit à l'autodétermination** plutôt que comme un droit de propriété (**proposition n° 1**)[1]. La reconnaissance du droit de propriété ne permettrait pas en effet 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...), 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**).

2. Renforcer les pouvoirs des individus 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**) ;

- de 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**) ;

- de **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, définition des critères de retrait de contenus licites en termes clairs, accessibles à tous et non discriminatoires (**proposition n° 6**).

- d'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 :

- création d'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**) ;

- mise en ***Open Data*** par la CNIL de toutes les **déclarations et autorisations** de traitements de données (**proposition n° 9**) ;

- développement de 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**) ;

- attribution 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] La liste des propositions de l'étude annuelle du Conseil d'État figure en partie V du présent document.

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 » (**propositions n° 13 et 14**) ;

- 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**) ;

- 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 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**).

• *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**).

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, ou « *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'*Open Data* aux collectivités territoriales, dont l'action en la matière est aujourd'hui inégale. Toutefois, la voie du droit souple apparaît plus appropriée pour promouvoir le développement de l'***Open Data***, 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, qui 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 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 oeuvre effective des dispositions qui le régissent (**proposition n° 35**), les contrôles successifs de la CNIL ayant montré un taux très élevé d'erreurs et d'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 oeuvre, 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 *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...) (**proposition n° 40**).

Il est proposé de faire de la 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**).

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 LCEN, 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 l'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**).

II. ELEMENTS DE REFLEXION…

1. … sur la protection des données personnelles

Un droit de propriété des personnes sur leurs données *vs* 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 dernier 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 (proposition n°1 de l'étude annuelle), c'est-à-dire *« le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel ».*

Le Conseil d'Etat 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'Etat 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 bien sûr, 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. Les délais de mise au point des directives ou règlements peuvent être longs et impliquer, par conséquent, **des initiatives des autorités françaises en matière, par exemple, de protection des données personnelles, de garanties en faveur des organes de presse ou encore de 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 »[2] 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 12 millions de fiches[3]. 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).

En 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

[2] Programme américain de surveillance des communications électroniques dont l'existence a été révélée le 6 juin 2013.
[3] Ce chiffre recouvre cependant des « doubles comptes » (la même personne peut être comptée deux fois), en raison de la fusion des fichiers d'antécédents de la police nationale (STIC) et de la gendarmerie nationale (JUDEX) qui a donné lieu au TAJ.

blancs de 2008[4] et de 2013[5] en ont fait une priorité, en prévoyant une augmentation des moyens alloués aux services de renseignement afin de mieux faire face aux nouvelles menaces contre la sécurité nationale, notamment celles 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[6]. 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 **l'arrêt *Digital Rights Ireland* de la CJUE**. Ce dernier 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 » [7] ; 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'Etat 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 n°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 les finalités de ces interceptions et en prévoyant leur contrôle par une autorité administrative indépendante (proposition n°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'Etat pour autoriser les traitements effectués à des fins de recherche dans le domaine de la santé ;

[4] *Livre blanc sur la défense et la sécurité nationale*, 17 juin 2008, La documentation Française, Paris
[5] *Livre blanc sur la défense et la sécurité nationale*, 19 avril 2013, La documentation Française, Paris
[6] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.
[7] Les « métadonnées » sont les données relatives à une communication électronique autre que son contenu : elles recouvrent notamment les informations permettant d'identifier les personnes ayant communiqué (numéro de téléphone, adresse électronique, etc), la durée de leur communication et leur localisation.

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.

2. … 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 »[8], les sites de partage de contenus[9] et les places de marché[10], bref 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[11], 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 celui-ci : 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 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 *e-Bay* 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, musique, photos, documents …), 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*[12], la CJUE a appliqué le même critère du « *rôle actif* » ; tout en laissant au juge

[8] L'écosystème d'applications recouvre à la fois le support sur lequel les applications peuvent être fournies (par exemple les systèmes d'exploitation pour téléphone mobile *iOS* d'*Apple* et *Android* de *Google* ou le réseau social *Facebook*), l'interface de programmation (souvent qualifiée « *d'API* », pour « *Application Programming Interface* ») mise à disposition des tiers pour qu'ils développent leurs applications et le « *magasin d'applications* » (*AppStore* pour *Apple* et *Google Play* pour *Google*), par lequel les utilisateurs du support pourront accéder à celles-ci.

[9] Comme *Youtube*, *Dailymotion*, *Instagram* ou encore les réseaux sociaux.

[10] Comme *Amazon*, *eBay* ou Leboncoin pour la vente de marchandises ou *AirBnB* pour la location d'appartements.

[11] Conseil national du numérique, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014.

[12] Lorsque l'internaute formule une requête sur *Google*, il reçoit d'une part les résultats de la recherche « *naturelle* », dans l'ordre défini par l'algorithme de *Google*, d'autre part les résultats des sites ayant acheté sur AdWords des mots-clés

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 Ch., 23 mars 2010, *Google France et Google Inc c/ Louis Vuitton Malletier*, C-236/08, § 115)[13]. 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 TGI 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[14]. 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.

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, en complément des acteurs habituels.

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

correspondant à sa recherche. La question de la qualification du service AdWords se distingue donc de celle de la qualification du service de recherche naturelle.

[13] À la suite à 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 .

[14] *Mosley c/ Google Inc*, n° 11/07970.

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.

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[15]. 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 la 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 desdites 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 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 du *net*, un fournisseur d'accès doit traiter de la même manière tous les sites internet ; un tel traitement égalitaire ne peut être demandé à un moteur de recherche, puisque l'objet même d'un moteur de recherche est de hiérarchiser les sites internet. Les plateformes n'ont pas une responsabilité analogue à celle des gestionnaires d'infrastructures d'un réseau qui doit être universellement accessible : elles peuvent, dans le cadre de leur liberté contractuelle, exercer une sélection des services proposés. Leur liberté éditoriale, consistant à proposer le classement 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 du Conseil d'État propose donc de soumettre cette nouvelle catégorie juridique à une exigence de **loyauté,** tant à l'égard des utilisateurs finaux 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 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 n°6) :

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

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

[15] Cf. le rapport précité du Conseil national du numérique sur la neutralité des plateformes.

3. … 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[16].

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[17].

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-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.

---

[16] 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 vs 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* ».

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

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[18]. 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 1* » 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* »[19]. 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 1* ») 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 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

[18] Cf. p. ex. M.-L. Niboyet et G. Geouffre de la Pradelle, Droit international privé, L.G.D.J, 2013.

[19] 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* ».

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 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 LCEN, 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[20]. 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, d'un acte de droit dérivé. En 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.

[20] Cf. notamment le rapport du groupe interministériel présidé par Marc Robert sur la cybercriminalité.

III. SELECTION DE JURISPRUDENCES

- **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 quand 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 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 ».

- **TGI Paris, 17e ch., 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-clé 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 L32- 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 MOSELEY 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§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 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 ; […] ».

■ CJUE, Gde Ch., 8 avril 2014, *Digital Rights Ireland et al.* et *Michael Seitlinger et al.*, C-293/12 et C-594/12.

« […] 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, paragraphe 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, arrêt Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 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, § 48; Rotaru c. Roumanie [GC], n° 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), n° 54934/00, § 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. »

Conseil d'État, 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 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 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 ; »

CJUE, Gde Ch., 13 mai 2014, *Google Spain c/ AEPD*, C-131/12

« (…) 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, paragraphe 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, 5e section, 18 septembre 2014, Brunet contre France, *requête n° 21010/10*

«[…] 1. L'existence de l'ingérence

1. La Cour constate d'emblée que l'inscription au 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.

2. 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*, n° 19522/09, § 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], n° 24876/94, § 104, 18 janvier 2001, et *S. et Marper c. Royaume-Uni* [GC], nos 30562/04 et 30566/04, § 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, § 49, série A n° 28, *Smith et Grady c. Royaume-Uni*, nos 33985/96 et 33986/96, § 88, CEDH 1999-VI, *Gardel c. France*, n° 16428/05, *B.B. c. France*, n° 5335/06, et *M.B. c. France*, n° 22115/06, 17 décembre 2009, respectivement §§ 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*, n° 66746/01, § 82, 27 mai 2004, et *S. et Marper*, précité, § 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], n° 44362/04, § 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, § 103, *Gardel c. France*, précité, § 62, CEDH 2009, et *M.K. c. France*, précité, § 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, § 119, et *B.B. c. France*, précité, § 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, § 122, et *M.K.*, précité, § 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, § 22, et *M.K.*, précité, § 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, § 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'Evry 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 (paragraphe 19 ci-dessus). 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 ; »

La notion d'autodétermination informationnelle (*Informationnelle Selbstbestimmung)* : Analyse de la cellule de droit comparé du CRDJ du Conseil d'État

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'Etat 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***[21] (« 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.

- 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'Etat 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[22], 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.

[21] 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). Etaient 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.

[22] *« 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.

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.

A. 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 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)*.

B. 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.

C. 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 24 janvier 2012 *Kontostammdaten BVerfG* 118,168).

IV. LEXIQUE

Algorithme : Programmes informatiques permettant de parcourir de grandes quantités de pages, 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 200 signaux ou indices permettant de trouver les réponses adéquates aux recherches des utilisateurs. On y trouve entre autres les termes figurants sur les pages web 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* ».

Big data : 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…) et non structurées sous forme de bases de données. La commission de terminologie et de néologie retient le terme « mégadonnées ».

***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 Web donné les habitudes et préférences exprimées par l'internaute lors d'une ou plusieurs visites de manière à lui proposer à nouveau des préférences exprimées lors d'une visite ultérieure.

Crowdfunding : Technique de financement, principalement des start-up, consistant à rechercher auprès de milliers de personnes les ressources nécessaires à la phase d'amorçage des projets de ces start-up.

***Crowdsourcing* (externalisation ouverte ou 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 *Google Spain c/ AEPD* de la Cour de justice de l'Union européenne du 13 mai 2014.

Diffusion en flux (« *streaming* ») : 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.

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. Pour ce faire, 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. A titre d'exemple, la société e-Bay a reçu la qualification d'éditeur par la CJUE 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 : Un *« fab lab »* (contraction de l'anglais « *fabrication laboratory* » ou « laboratoire de fabrication en français) est un 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 Web conçus et gérés par des tiers. Les internautes peuvent ainsi avoir accès au contenu déposé 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 marché 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 courses* » ou « MOOCs » : En français, 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 *Web* 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 : Logiciel informatique permettant l'accès à internet. Le terme anglais pour « navigateur internet » est « *web browser* ».

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 quel que soit leur contenu. 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 » également appelés « 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 8 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 : Désigne une orientation de politique publique ayant pour objet de rendre accessibles à tous via le web 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)** : 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 PNR 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 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, 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 *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 : 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'UE vers les Etats-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 internet en haut débit.

Spam : Pour la CNIL, le « *spamming* » ou encore le « *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.

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 *Web*.

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 des pages sur les 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.

V. RECAPITULATIF DES MESURES PROPOSEES

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 : Anticiper 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° 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.

VI. BIBLIOGRAPHIE SELECTIVE

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.
J. JARVIS, *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-LOFSKOG 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.

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., BENISTI 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 EUROPEENNE, 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'ETAT, *Internet et les réseaux numériques*, La Documentation Française, 1998.
CONSEIL NATIONAL DU NUMERIQUE, *Citoyens d'une société numérique*, novembre 2013.

CONSEIL NATIONAL DU NUMERIQUE, *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 RAUDIERE 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'Etat à la Réforme de l'Etat*, 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., FAUGERE J.-P., FLICHY P., *Administration électronique et protection des données personnelles*, Livre blanc, février 2002.
URVOAS J.-J ET VERCHERE P., *Mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, Assemblée nationale, mai 2013.
URVOAS J.-J., P. VERCHERE 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.

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 Etats-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, no.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.
JACQUE 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*, 06 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 Etats-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.

Textes normatifs

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.**

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.

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).

Décisions

CJCE / CJUE

CJCE, C-325/85, 15 décembre 1987, *Irlande c/ Commission*, C-325/85

CJCE, C-262/88, 17 mai 1990, *Barber*

CJCE, C-7/97 26 novembre 1998, *Oscar Bronner c/ Mediaprint*

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

CJUE, C-275/ 06 ,29 janvier 2008, *Promusicae c/ Telefonica*
CJUE, C-236/08, Gde Ch., 23 mars 2010, *Google France et Google Inc c/ Louis Vuitton Malletier*
CJUE, C-92/09 et C-93/09, Gde Ch., 9 novembre 2010, *Volcker und Markus Schecke GbR et Hartmut Eifert*
CJUE, C-858/08, Gde Ch., 7 décembre 2010, *Pammer et Hotel Apenhof*
CJUE, C-324/09, Gde Ch., 12 juillet 2011 *L'Oréal c/ e-Bay*,
CJUE, Gde Ch., 25 octobre 2011, *eDate Advertising*
CJUE, C-70-10, 24 novembre 2011, *Scarlet c/ SABAM*
CJUE, C-360/10, 16 février 2012, *SABAM*
CJUE, C-523/10, 19 avril 2012, *Wintersteiger*
CJUE, C-617/10, Gde Ch., 26 février 2013, *Åklagaren c/ Hans Åkerberg Fransson*
CJUE, C-170/12, 3 octobre 2013, *Pinckney c/ Mediatech*
CJUE, C-314/12, 27 mars 2014 *UPC Telekabel*
CJUE, C-293/12 et C-594/12, 8 avril 2014 *Digital Rights Ireland et al.* et *Michael Seitlinger et al*
CJUE, C-131/12, 13 mai 2014, *Google Spain* c/ AEPD

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

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'Etat

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'Etat, 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

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, *e-Bay contre Société Parfums Christian Dior et autres*, n°11-10.508
Cass. Civ 1re, 12 juillet 2012, *Auféminin.com et Google France*

Cass. Com., 25 juin 2013, n° 12-17.037

Cour suprême des Etat-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, p. 1 et s. (Arrêt sur le recensement, *« Volkszählungsurteil »*).

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.

TGI de Paris

TGI Paris, 3 novembre 1998, *UNADIF c/ Faurisson*,

TGI Trib. Corr. Paris, 26 février 2002, *Yahoo !*

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

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 oeuvre 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

Ce document a été préparé
par la section du rapport et des études
du Conseil d'État