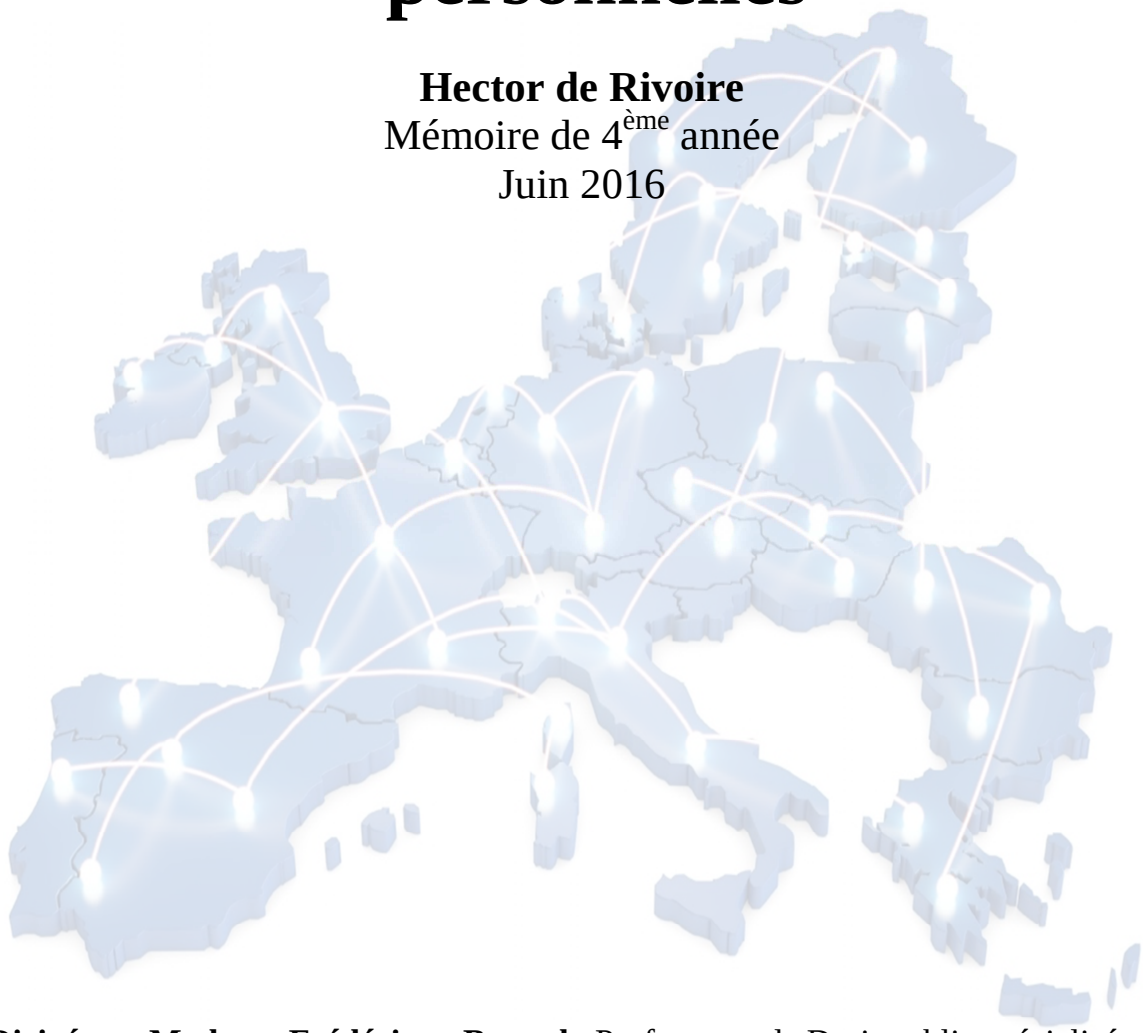
Institut d'Etudes Politiques de Strasbourg

Le marché intérieur du numérique à l'épreuve de la protection des données personnelles

Hector de Rivoire

Mémoire de 4ème année

Juin 2016



Dirigé par Madame Frédérique Berrod, Professeure de Droit public spécialisée dans le droit de l'Union à l'Institut d'Études Politiques et à l'Université de Strasbourg

L’université de Strasbourg n’entend donner aucune approbation ou improbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à leur auteur.

Remerciements :

Je remercie vivement Madame le Professeur Frédérique Berrod, pour sa patience et sa disponibilité dans la direction de ce mémoire, et l'intérêt qu'elle a manifesté à ce sujet d'étude. Je remercie également Madame le Professeur Catherine Ledig, qui a accepté de codiriger cette soutenance.

Je remercie également Fréderic Donck et Maarit Palovirta, qui ont encadré mon stage à la Internet Society en juin-juillet 2015, et m'ont donné le goût des enjeux numériques européens.

Je remercie enfin mes parents et mes grands-parents pour le savoir qu'ils m'ont transmis, eux qui ont le mérite d'avoir étudié alors que Wikipédia et Google n'existaient pas.

« La retraite est révolte. Gagner sa cabane, c'est disparaître des écrans de contrôle. L'ermite s'efface Il n'envoie plus de traces numériques, plus de signaux téléphoniques, plus d'impulsions bancaires. Il se défait de toute identité. Il pratique un hacking à l'envers, sort du grand jeu. »

Sylvain Tesson, « *Dans les Forêts de Sibérie* », Paris, Gallimard, 24 avril 2013

Table des abréviations :

ICT : Informations and Telecommunications Technologies

CJCE : Cour de Justice des Communautés Européennes

CNIL : Commission National de l'Informatique et des libertés

DUDH : Déclaration Universelle des Droits de l'Homme de 1948

CEDH : Convention Européenne de sauvegarde des droits du citoyens et des libertés fondamentales de 1950

CEDH : Cour Européenne des Droits de l'homme

CEPD : Contrôleur Européen de la protection des données

GAFA : Google, Apple, Facebook, Amazon

NATO : Netflix, Airbnb, Tesla, Uber

SAFE HARBOUR : Accord regroupant un ensemble de principes de protection des données.

SWIFT : accord Etats-Unis-Union Européenne sur la protection des données

G29 : association des autorités de régulations et de protection des données

MOOC : Formation en ligne ouverte à tous

CLOUD : « Informatique en nuage », désigne l'utilisation de seveurs de stockages distants

EEE : Espace Economique Européen

TUE : Traité sur l'Union Européenne

TFUE : Traité sur le Fonctionnement de l'Union Européenne

PRISM : Programme de Surveillance de la NSA

DNS : Système de noms de domaine internet

Plug-In : Elément à ajouter sur logiciel pour obtenir de nouvelles fonctionnalités

Lexique :

Données à caractère personnel : toute information concernant une personne physique identifiée ou identifiable

Fichier automatisé : tout ensemble d'informations faisant l'objet d'un traitement automatisé

Sommaire

Résumé :

Le présent mémoire vise à éclairer le lecteur sur les conséquences de la protection des données personnelles sur le marché intérieur du numérique et ses acteurs. En étudiant la construction par le législateur européen d'un régime de protection des communications électroniques et des informations personnelles, dans un contexte d'inflation de la cyber surveillance et de gouvernance éclatée d'Internet, ce mémoire vise à montrer que malgré les risques qu'elle présente, la donnée demeure une ressource économique indispensable au bon fonctionnement du marché intérieur. Partant de ce postulat, bien qu'il y ait un impératif d'intervention étatique dans le secteur du numérique, les législateurs doivent opérer une conciliation entre libertés fondamentales et compétitivité des acteurs.

Asbtract :

This master thesis intends to inform the reader on the consequences of the data protection on the European digital market and its actors. By studying the implementation of a legal regime of protection of the electronic communications and the personal data by the European legislator, in a context of inflation of cyber-surveillance and fragmented governance of Internet, this report aims to show that in spite of the risks which it presents, the data remains an economic resource which is essential to the smooth functioning of the internal market. Leaving of this postulate, although there is an imperative of state intervention in the sector of digital technology, the legislators have to operate conciliation between fundamental liberties and competitiveness of the actors.

Introduction :

Lorsqu'on réfléchit aux implications de la révolution impulsée par le numérique dans l'ensemble des secteurs traditionnels, on ne peut qu'approuver la thèse de Gilles Babinet, ancien président du Conseil National du numérique et *serial entrepreneur*, qui estime que la révolution actuelle pourrait compter parmi les trois grandes inflexions qu'a connue l'humanité. Accélérant l'histoire comme l'invention de l'écriture par la civilisation sumérienne et l'invention de l'imprimerie par Gutenberg, cette révolution digitale représente, selon l'auteur de « *L'ère numérique, un nouvel âge pour l'humanité* »[1], une rupture de paradigme majeur pour l'ensemble de notre civilisation. Formidable incubateur de bien être et outil de progrès, le numérique est à la fois un levier de développement puissant, et un outil de surveillance d'une redoutable efficacité. Permettant aussi bien la distribution massive du savoir et des techniques de santé que la transformation des problématiques de vie privé, il appelle à une véritable prise de conscience de la part des institutions, qui doivent réguler ce nouveau secteur, autant pour créer les conditions du profit que pour protéger leurs citoyens. Benoît Thieulin, autre ancien président du Conseil National du Numérique, a insisté sur cette nécessité lors d'une conférence à la Maison de l'Europe, le 18 février 2016 : grâce à l'incubation des données, les progrès numérique nous permettent de savoir mètre par mètre comment nous nous déplaçons depuis que nous sommes munis d'un portable[2]. Il présuppose également sans trop de risques qu'un dictateur tel que Staline, qui avait installé le contrôle des communications par l'ouverture des courriers n'aurait jamais rêvé d'un tel pouvoir. Ce phénomène du « Big Data », peut s'apparenter à un autre phénomène, de la même famille, celui du « Big Brother ». Dans le premier cas, on s'interroge sur l'identité de la personne qui nous surveille, dans le second, sur l'utilisation des ressources de la surveillance : les données.

Pour donner au lecteur un aperçu de cette révolution par le Big Data, il est essentiel de lui donner quelques chiffres. D'après l'agence « We are Social », commissionnée pour ce travail par le bureau du tourisme de Singapour, sur une population mondiale atteignant 7,416 milliards en 2016, 3,419 milliards sont utilisateurs d'Internet, 2,430 milliards peuvent être considérés comme utilisant activement les réseaux sociaux et 4,730 milliards utilisent un

[1] Babinet, Gilles « *L'ère numérique, un nouvel âge de l'humanité, cinq mutations qui vont bouleverser notre vie* » Broché, 23 janvier 2014
[2] Thieulin Benoît, Discours sur l'Europe du numérique à la Maison de l'Europe, 18 février 2016

téléphone mobile. Les réseaux sociaux, formidables incubateurs de savoir rassemblent des communautés sans cesse plus importantes d'utilisateurs. En 2016, Facebook en compte 1,55 milliards, Instagram 400 millions, Twitter 307 millions, LinkedIn 100 millions, tandis que les applications de messagerie permettent une interconnexion toujours plus importante ! Skype rassemble 300 millions d'usagers, Whatsapp et Facebook Messenger 800 millions chacun, infléchissant considérablement la courbe des communications électroniques. [3] Loin de se limiter aux pays les plus développés, le numérique est un outil actuellement largement utilisé par de nouveaux acteurs de l'économie mondiale tels que le Brésil, l'Argentine et même les Philippines, dont les citoyens passent respectivement en moyenne 3,3 , 3,2 et 3,7 heures en moyenne sur les réseaux sociaux par jour, devançant largement la France (1,3) et l'Allemagne (1.1). [4] Ces chiffres montrent l'importance croissante que prend la donnée dans nos vies quotidienne, faisant souvent office de « facilitateur ». Pour le secteur de l'assurance, les données symbolisent une possibilité d'indexer les tarifs aux données des utilisateurs ; pour les banques, un moyen de sécuriser les prêts en se renseignant sur les futurs emprunteurs. Les services municipaux de la ville de New York disposent de données déterminantes sur les immeubles risquant l'incendie. Cette utilisation des données à outrance crée également de nouveaux besoins. La Suisse se transforme peu à peu en coffre fort numérique, hébergeant une masse considérable de serveurs de clients inquiets sur l'utilisation de leurs données personnelles. A la fois outil puissant et incontournable, et redoutable instrument de surveillance, le Big Data provoque de nombreuses questions dans le débat public. Entre réglementations jugées trop lourdes, les dispositifs d'autorégulation perçus comme des recettes libérales, et la régulation approximative, les Etats ont la main qui tremble lorsqu'il faut intervenir dans se secteur, dont le poids dans la croissance et la technicité des enjeux sont des freins considérables à l'action des législateurs du monde entier.

Pourtant lorsque Edward Snowden, un jeune informaticien de la CIA, attire l'attention du monde sur les programmes de surveillance de masse américains et britanniques, il insère durablement la question de l'utilisation des donnés au cœur du débat public, et amène les Européens à une brutale prise de conscience de la faiblesse de leurs moyens, et de la fragilité des protections qui les entourent. Comme le proclamait Benoît Thieulin, l'Union Européenne découvre à l'heure actuelle, 30 ans après les Etats-Unis, ce qui va faire la puissance du XXIe siècle. Les attributs de la puissance, longtemps traditionnels et rivés sur les complexes

[3] Kemp, Simon « *The social traveller* », We are Social, 18 avril 2016 p8-15
[4] Ibid

militaro-industriels, sont en train de glisser vers des infrastructures de réseaux et la maîtrise des données[5]. La chute du mur de Berlin avait à l'époque marqué les consciences américaines, et déterminé le choix de politiques publiques résolument favorables à l'émergence de géants du numérique. La libéralisation du GPS en 1989, la défiscalisation de l'investissement dans le numérique en 1998, et la tentative d'un traité Safe Harbour avec l'Union Européenne démontrent l'asymétrie de la prise de conscience de part et d'autre de l'Océan Atlantique. Les divisons des Etats Membres, qui placent rarement leurs revendications du côté de la protection des citoyens face à la perspective d'une restriction des libertés économiques, sont révélatrices de l'incapacité de l'Europe à rassembler les 28 Etats-Membres autour d'une position commune forte et cohérente pour construire un véritable *Habeas Corpus Européen du Numérique*[6]. Ceux-ci, en accord sur l'approfondissement du marché intérieur par la suppression progressives barrières à la libre circulation des biens, des personnes, des services et des capitaux, sont nettement plus divisés sur des enjeux aussi importants que la consolidation de la protection de la propriété intellectuelle, l'harmonisation fiscale et la protection des droits fondamentaux. Par ailleurs, les tergiversations européennes servent considérablement les Etats-Unis dans les négociations transatlantiques, qui cherchent à imposer à l'Union Européenne des modèles souples et modernes d'autorégulation, destinés en ce qui concerne les données personnelles à déléguer leur protection aux acteurs privés.

Cependant à l'élection de Jean Claude Juncker à la tête de la commission européenne, le 15 juillet 2014, succède un agenda porteur d'une authentique volonté de changement. En effet le marché unique du numérique se retrouve propulsé à la deuxième place des dix priorités de la Commission Européenne, devançant les questions d'environnement et d'énergie. Le nouveau président de l'institution n'avait alors pas fait mystère de son ambition en proclamant dans son discours à Paris le 27 octobre que « *Le numérique, c'est notre nouvelle révolution industrielle, celle dont doit profiter un secteur industriel qui en Europe aujourd'hui représente 2 millions d'entreprises et 33 millions d'emplois* ». Il avait également rappelé l'importance du progrès des technologies numériques « *essentielles à la productivité et à la compétitivité de l'industrie européen* », étant des instruments de modernisation des schémas de production et de commercialisation des entreprises. [7] Au delà des enjeux

[5] Thieulin Benoît, Discours du au forum annuel de Trans Europe Experts, 21 mars 2016
[6] Annexe 1
[7] Juncker Jean-Claude « Construire l'Europe industriel du numérique » discours prononcé le 27 octobre 2015

économiques entourant cette priorité, la Commission Juncker a à cœur de construire une véritable protection des données des citoyens de l'Union. Il répond ainsi à une inquiétude latente exprimée par ceux-ci dans différents sondages de l'Eurobaromètre : 67% des européens avaient ainsi déclaré être préoccupés par la possibilité que leurs données sont utilisées dans des buts différents que ceux au nom duquel elles avaient été collectées. Seuls 15% de ces mêmes citoyens estimaient par ailleurs avoir un réel contrôle des informations qu'elles décidaient de mettre en ligne, et 30% qu'ils n'avaient pas de contrôle du tout[8]. Au delà de la défiance des Européens pour l'efficacité des dispositifs réglementaires actuellement en vigueur, ceux-ci appellent à un véritable changement en déclarant unanimement la nécessité d'être informés sur la perte ou le vol de leurs données, et en se déclarant favorable à 90% à l'application des mêmes droits en matière de protection des données dans l'ensemble de l'Union Européenne. [9] Pour répondre à ces préoccupations, le législateur européen fait face à un double enjeu, à la fois européen et transatlantique. Concernant ce dernier, la Commission Européenne à présenté le 29 février 2016 les textes instaurant le bouclier de protection des données UE-US, comprenant les principes du « *Privacy Shields* » auxquels les entreprises doivent adhérer, ainsi qu'une série d'engagements écrits du gouvernement des États-Unis touchant à la mise en œuvre du dispositif, en particulier concernant des assurances sur les garanties et les conditions d'accès des pouvoirs publics aux données.[10] Concernant l'enjeu européen, l'accord politique intervenu lors du trilogue, début 2016 devrait mener à une véritable réforme de la protection des données. Celle-ci actualiserait et remplacerait les règles actuellement en vigueur en matière de protection des données, qui se fondent sur la directive sur la protection des données de 1995 et la décision cadre de 2008 pour le secteur de la police et de la justice pénale. Cependant, l'agenda numérique 2020 de la Commission ne se limite pas à vouloir sécuriser les droits des citoyens. Révélant aussi bien les divisions des Etats-Membres que la volonté de la Commission de faire du numérique le fer de lance de sa stratégique économique, celle-ci propose une réforme globale. En régulant des pans entiers du secteur, comme la concurrence dans les télécoms, le commerce électronique et ses développements transfrontaliers, et la protection des données personnelles, les législateurs prétendent faire face à la fois aux dysfonctionnements du géo-blocage, répondre aux

[9] Eurobaromètre 431 « Data Protection » p9-11

[10] Communication de la Commission Européenne « La Commission européenne présente le paquet «bouclier de protection des données UE-États-Unis» 29 février 2016 à Bruxelles

inquiétudes des entreprises et des citoyens sur l'utilisation de leurs données, et créer les conditions d'émergence d'écosystèmes numériques. Cette dernière problématique se retrouve plongée au cœur du débat sur l'émergence d'un marché unique du numérique, qui serait « européen », et dans l'idéal, dominé par des entreprises européennes. Par un communiqué de Presse le 25 mars 2015, Andrus Ansip et Günther Oettinger, respectivement vice président pour le marché unique numérique et commissaire pour l'économie et la société numérique, ont martelé l'importance de l'émergence d'un « *marché européen qui permette à de nouveaux modèles économiques de s'épanouir, aux start-ups de se développer et à l'industrie de tirer parti de l'internet des objets* ».[11] La Commission s'engage ici dans un chemin sinueux, à la croisée des problématiques de concurrence, de protection des données, de libre circulation de ces mêmes données, et de renforcement des plateformes européennes du e-commerce. L'objectif est extrêmement clair : faire tomber les frontières numériques des 28 Etats Membres, et faire face à la domination écrasante des géants américains communément appelés GAFA, sur les marchés européens.. La commission s'attaque à des objectifs difficiles : le numérique n'est pas un secteur comme les autres, il regroupe les plateformes qui supportent, conditionnent, et développent l'économie mondiale. Les GAFA, Google, Apple, Facebook et Amazon pèsent ensemble 1675 Milliards dollars, plus que la totalité des entreprises du CAC 40[12]. Google, créé en 1998 capte à l'heure actuelle 94% du marché de la recherche en ligne en Europe, et Facebook, le plus grand média du monde, dispose de près de 260 millions d'utilisateurs sur le continent, plus encore qu'aux Etats Unis. Quand à Amazon, la plateforme est encore leader mondial de l'e-commerce, tandis que le système d'exploitation de Microsoft domine le secteur informatique. Selon Eric Sadin, auteur de *La vie algorithmique,* « *ce qui lie les GAFA, c'est une vision du monde, plus encore que de vendre des services, il s'agit de conduire les existences et d'instaurer un assistanat algorithmique de nos vies* »[13]. Lorsque Google choisi de faciliter la pré-installation de ses applications sur les mobiles Android ou de créer les Google Glass, lorsque Apple lance son modèle de montre, ces entreprises cherchent avant tout à créer une « *vision d'accompagnement de l'existence* »[14] , en émaillant par leurs produits notre quotidien. Les nouveaux acteurs de ce secteur, les

11 Communication de la Commission Européenne « Stratégie pour le marché unique numérique: la Commission européenne définit les grands domaines d'action » 25 mars 2015 à Bruxelles

[12] Vandecasteele, Mylène « L'économie des GAFA est maintenant aussi importante que celle du Danemark » L'Express Business, 28 juillet 2015

[13] Sadin Eric « La vie algorithmique : critique de la raison numérique » Broché, 12 mars 2015

[14] Ibid

NATU, Netflix, Airbnb, Tesla et Uber sont en réalité entièrement dépendant des plateformes d'échanges, qui stimulent considérablement l'économie européenne. Face aux ambitions européennes, notamment en ce qui concerne la protection des données personnelles, et la volonté de restriction de leurs collectes, ces entreprises voient leur avenir s'assombrir et leurs dépenses en lobbying augmenter. Par ailleurs, la gouvernance d'Internet, dont l'équilibre est centré sur l'ICANN, société de droit californien, est sans cesse remise en question. En effet, l'ONU, par la Commission Européenne, les Etats pointent les liens entre l'organisation qui assure la régulation des noms de domaines et le Département de Commerce américain, qui a pour objectif affiché depuis Bill Clinton d'imposer au reste du monde une vision libérale de la donnée, en déléguant laissant aux entreprises le soin de protéger les informations personnelles de leurs clients.

Si à l'heure actuelle Internet a déjà atteint un très haut degré de pénétration au sein de la majorité des pays européens, ce n'est pas le cas pour les pays d'Asie Centrale et pour une partie de l'Europe de l'Est, où le développement de standards, de points d'échanges de réseaux et de la 3G sont encore de vastes chantiers en négociation avec les gouvernements locaux. Au sein de l'Union Européenne, les Etats-Membres se trouvent presque exclusivement à un deuxième niveau de réflexion, qu'on peut illustrer par la question suivante : comment, maintenant que nous disposons tous d'internet, du réseau 3G, d'un téléphone cellulaire, choisissons nous de gérer ces nouvelles libertés ? Comment articulons nous un besoin de sécurité croissant, la conservation de ces libertés par les utilisateurs, et la protection de leurs données personnelles ? Malgré les ambitions de la Commission Juncker, de nombreuses questions manquent à l'appel des priorités, comme la question des droits d'auteur, la cybercriminalité, l'économie collaborative, la numérisation dans l'industrie, la robotique, et une vision à long terme de la gestion du bien communs. Trop souvent, c'est la Cour qui défend, jurisprudence après jurisprudence, les droits des consommateurs. La Commission, exécutif aux ordres du Conseil, a vu ses ambitions considérablement réduites par la pression des Etats-Membres, et ses objectifs diminués.

Problématique:

On peut alors s'interroger sur la difficulté du législateur à équilibrer les besoins des entreprises du secteur, véritable fer de lance de ce que Rifkine appelle la *« troisième révolution »*[15] et acteurs du marché intérieur du numérique, avec la construction d'une doctrine européenne de la protection des données.

Dans une première section, je montrerai la nécessité pour les législateurs d'opérer une transition de la protection de la vie privé des citoyens, donc de leur données personnelles, vers un véritable droit pour ces mêmes citoyens à l'accès de leurs données. Je montrerai dans une première partie que c'est un enjeu qui s'inscrit dans la protection des droits et libertés fondamentales, d'abord autour de traités internationaux, puis de la mise en place de textes européens encadrant l'utilisation de la donnée. Je justifierai par la suite la mutation du droit de l'Union Européenne, oscillant entre dispositifs de réglementation et systèmes d'autorégulation. En effet, celui-ci a consacré progressivement une batterie de nouveaux droits pour le citoyen, dans un contexte où la donnée est devenue l'arme des gouvernements pour mettre en place la cyber-surveillance. Enfin dans une troisième partie, j'expliquerai l'approche originelle de régulation de l'Internet, centrée à la fois sur la théorie de l'économie des communs, et sur une gouvernance ouverte et originale.

Dans une deuxième section, je montrerai que le bon fonctionnement du marché intérieur est conditionné à la libre circulation de la donnée, véritable ressource économique de ce marché. En premier lieu j'aborderai la nécessité d'une intervention étatique dans ce secteur, en expliquant l'impératif d'une approche pluridisciplinaire du législateur sur le sujet, accompagnant efficacement le e-commerce. J'insisterai également sur les carences de l'agenda numérique de la Commission, malgré les avancées notables sur des sujets aussi importants que le geo-blocking et le cloud couputing. En second lieu, je démontrerai que la difficulté pour le législateur européen réside dans l'équilibre à trouver entre la préservation des libertés fondamentales et la compétitivité des acteurs. En effet, la Commission utilise le droit de concurrence comme un instrument économique de sa stratégie européenne consistant à faire émerger les entreprises européennes du numérique.

[15] Rifkine, Jeremy « *La troisième révolution industrielle* » Babel, 28 septembre 2013

Section I : La nécessaire transition entre protection des données et droit d'accès

Bien avant l'apparition d'Internet, deux anciens étudiants de la Law School de Harvard, Samuel D. Warren et Louis Brandeis ont publié en 1890 un article dans la revue de droit de Harvard, considéré encore aujourd'hui comme le texte fondateur de la vie privé. Intitulé « The Right to Privacy », cet texte réclamait le droit pour les personnages publics « d'être laissé seuls » par la presse à sensation[16]. Précisant que « Now the right to life has come to mean the right to enjoy life, the right to be let alone (…) and the term proprerty has grown to comprise everey form of possession-intangible as well ass tangible ». [17] Par ce texte, les deux juristes ont fait figure de précurseurs en terme de reconnaissance du droit à l'image mais aussi en terme de propriété immatérielle, évoquant sans s'en douter les débats houleux que nous connaissons aujourd'hui concernant sur les données. Concernant l'Union Européenne, on peut affirmer que la protection des données des citoyens s'est construite autour d'une grande diversité de sources, à la fois textuelles et jurisprudentielles. Cependant ce droit à connu une évolution, d'abord stricte autour du principe stricte respect de la vie privé, défini par la Convention Européenne des droits de l'homme à l'article 9 et la Convention 108 du conseil de l'Europe, puis une conception plus moderne l'émergence progressive d'un cadre juridique d'accès à la donnée, et enfin par un droit à l'oubli de celle-ci. Dans un contexte de cyber surveillance massive, où nous découvrons un nouveau Big Brother, dénoncé aussi bien par des lanceurs d'alerte tels que Edward Snowden ou Julien Assange que par des dirigeants d'entreprises comme Marissa Mayer, patronne de Yahoo! qui s'attaque « *au gouvernement tyrannique des Etats-Unis* » [18] , nous nous habituons progressivement à la réalité de la collecte de nos communications électroniques et de nos données aussi bien par des entreprises que par des états malveillants. Ce phénomène est aussi inquiétant que grisant, puisque d'une part il sous-entend que notre vie privé n'existe plus, que la neutralité du net est une fiction, et d'autre part, il donne à des individus un pouvoir considérable d'information, qui a permis à des lanceurs d'alerte d'altérer durablement le

[16] Warren Samuel et Brandeis Louis« *The Right to Privacy* » Harvard Law Review N°5, Vol IV, 15 décembre 1890
[17] Ibid
[18] Lacroix, Alexandre « *Faut-il avoir peur de la peur de la cyber-surveillance ?* » Philosophie Magazine, 20 septembre 2013

prestige des Etats-Unis. Dans cette partie nous étudierons en premier lieu la protection des données au sens traditionnel du terme, comme étant un enjeu s'inscrivant dans la protection des droits et libertés fondamentales, définies par les textes européens. Puis, nous montrerons que la Cour de Justice de l'Union européenne a progressivement dégagé un droit à l'oubli et un droit de protection des auteurs pour les citoyens européens. Par ailleurs, dans cette même partie, nous analyserons l'influence de la conjoncture et de la remise en question de la neutralité du net depuis 2001. Enfin, nous présenterons l'approche de la régulation d'Internet telle qu'elle fut pensée par ses fondateurs et en partie appliquée par les Etats-Unis, centrée sur la gestion de l'Internet, « bien commun » planétaire.

A. Un enjeu qui s'inscrit dans la protection des droits et libertés fondamentales :

1. Déclaration Universelle des Droits de l'Homme et du citoyen de 1948, article 12

Pour appréhender un enjeu aussi complexe, il est essentiel de faire un rappel chronologique des différents textes qui ont fondés la protection des données des citoyens. En effet, c'est à travers plusieurs phases que l'Union Européenne, répondant aux nécessités de l'Histoire, à forgée une position extensive, d'abord centrée autour de la protection de la vie privé, étendue par la suite à la vie privé sur Internet. Ainsi, le droit à la protection de la sphère privé d'un individu contre l'intrusion d'un tiers, en particulier d'un état à été pour la première fois énoncée à l'article 12 de la déclaration universelle des droits de l'homme rédigée en 1945 dans le cadre des Nations Unies, qui dispose que *« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »*. [19] Cet article, véritable sanctuarisation de la vie privé d'un individu, entoure celle-ci d'une protection que ni l'employeur, ni l'état ne peut atteindre. Cependant, cette déclaration étant une résolution de l'Assemblée Générale des Nations Unies, elle ne possède pas de portée juridique contraignante et ne peut être invoquée devant un

[19] Déclaration Universelle des droits de l'Homme, article 12, 10 décembre 1948

juge.[20] Le conseil d'Etat avait d'ailleurs rappelé lors d'un arrêt Roujansky de 1984 que la seule publication au Journal officiel du 9 février 1949, du texte DUDH « *ne permet pas de ranger cette dernière au nombre des textes diplomatiques qui, ayant été ratifiés et publiés en vertu d'une loi, ont aux termes de l'article 55 de la Constitution du 4 octobre 1958, une autorité supérieure à celle de la loi interne ; qu'ainsi, les requérants ne sauraient utilement invoquer cette déclaration pour contester la régularité du scrutin* »[21]. Cette résolution à la portée morale plus que juridique, a été complétée par deux pactes le 16 décembre 1966. Le premier, relatif aux droits civils et politiques, a repris au mot près les principes de l'article 8 de la DUDH en lui conférant une valeur juridique contraignante. L'article 17 dispose ainsi dans un premier point que « *Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.* », puis dans un second point que « *Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ». Cependant, c'est la convention européenne des droits de l'homme de 1950 qui a ouvert et facilité le recours à un juge pour les citoyens européennes en cas de violation de leurs libertés fondamentales. En effet le Traité de Rome signé le 4 novembre 1950, a institué l'existence d'une cour européenne des droits de l'homme dont le siège est à Strasbourg. [22]

2. Convention Européenne des droits de l'homme de 1950, article 8

Au lendemain de la deuxième guerre mondiale, le Conseil de l'Europe créée pour réunir les états sous les valeurs de la démocratie et pour promouvoir l'Etat de Droit, a adopté la convention européenne des droits de l'homme en 1950. Celle-ci ouvrait un droit au respect de la vie privé par l'article 8, en reprenant dans un premier point l'article 12 de la DUDH disposant que « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». Cependant, elle dispose également dans un second point qu'il « *ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour*

[20] Vie Publique « *La DUDH de 1948 et la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950* »
[21] CE, arrêt d'assemblée M. Roujansky et autres, 23 novembre 1984, considérant 5
[22] Vie Publique « *La DUDH de 1948 et la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950* »

autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. ». Cette convention apportait donc une batterie d'exceptions invocables par les états en cas de violation des libertés fondamentales, mais le droit à la protection et la collecte de données à caractère personnel fait partie du droit des citoyens eu respect de la vie privé et familiale, du domicile et de la correspondance. [23]

3. Convention 108 du Conseil de l'Europe : position originelle de l'UE sur la question

Dès les années 70, pour faire face à l'émergence des nouvelles technologies, le conseil des ministres du Conseil de l'Europe avait pris plusieurs résolutions comme celles de 1973 et 1974, relatives en l'espèce à la protection des personnes physiques vis a vis des banques de données dans le secteur public[24]. En 1981, les Etats Membres du Conseil de l'Europe ont signé le premier instrument international contraignant pour la protection des personnes à l'égard du traitement automatisé des données à caractère à personnel. Actuellement, l'information circule plus aisément que jamais, sans pour autant que ses usagers bénéficient des mêmes droits et de la même protection, L'objectif de la convention, énoncé dans son article 1 qui dispose que *« le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données)* »[25] est donc plus que jamais d'actualité. Ouverte à l'adhésion des Etats non membres du Conseil de l'Europe, elle regroupe les 28 Etats-membres de l'Union Européenne, les 45 pays membres du Conseil et deux pays non membres, l'Uruguay depuis

[23] Conseil de l'Europe et Agence des droits fondamentaux « Manuel de Droit Européen en matière de protection des données », Avril 2014, p16

[24] Conseil de l'Europe, Comité des Ministres, résolution (73)22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, 26 septembre 1973 ; Conseil de l'Europe, Comité des Ministres, résolution (74)29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, 20 septembre 1974.

[25] Conseil de l'Europe, Convention 108, article 1, 28 janvier 1981

2013 et le Maroc depuis 2014. Elle possède un champ d'application large, couvrant le secteur privé et le secteur public, y compris la police et la justice. Cette convention a d'une part pour objet de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel, et d'autre part pour but de proscrir le traitement des données « *sensible*s ». Dans cette catégorie, on retrouve les informations relatives à l'origine social à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle, aux condamnations pénales, en l'absence de garanties offertes par le droit interne[26]. Dans un contexte où il n'existait ni tablettes, ni ordinateurs portables, ni téléphones mobiles, ni réseaux sociaux, ni géolocalisation la Convention a également ouvert un droit pour les personnes concernées de connaître les informations stockées à leur sujet et d'exiger le cas échéant des rectifications. Elle crée donc un droit à l'information pour les citoyens européens, tout en rassurant les Etats quand aux restrictions possible de ce droit en cas de mise en cause de critères d'intérêt généraux comme la sécurité publique et la défense. Selon l'ancien Contrôleur Européen de la protection des données Peter Hustinx, il est clair que l'approche de cette Convention ne consiste pas à restreindre systématiquement le traitement des données à caractère personnel comme une atteinte aux droits fondamentaux, mais à le soumettre à certaines conditions juridiques comme le principe disposant que les données en question ne peuvent être traitées qu'à des fins légitimes et spécifiées[27]. En 2011 une consultation publique organisée pour moderniser la convention a permis de confirmer ses principaux objectifs, centrés sur le renforcement du droit au respect de la vie privé dans le domaine du numérique et sur l'amélioration du suivi de la cette convention. [28] Avant cette consultation, Jean-Philippe Walter, Président du comité consultatif de la convention 108, avait vivement encouragé les signataires lors du 30e anniversaire de la convention à ne pas intervenir en ordre dispersé à l'encontre de firmes comme Google ou Facebook, « *de peur d'affaiblir l'impact de la protection des données en Europe et dans le monde* »[29]. Il avait également insisté sur le « *potentiel unique* » de la Convention 108 « *pour devenir la norme majeure d'une législation universelle de protection des données* ». Cependant, les signataires de la Convention forment

[26] Conseil de l'Europe et Agence des droits fondamentaux « Manuel de Droit Européen en matière de protection des données », Avril 2014, p20

[27] Hustinx, Peter, CEPD «*Le droit de l'Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données*», article CEPD, 14 septembre 2015 p7

[28] Ibid p17

[29] Walter, Jean Philippe « *La convention 108-d'un standard européen vers un standard universel* ? » Exposé dans le cadre de la Conférence internationale sur la protection des données à Varsovie, 21 septembre 2011

un bloc majoritairement européen, on peut donc légitimement s'interroger sur l'universalité d'une telle norme, qui ne relève pas nécessairement de la conception américaine de la protection des données.

4. Directive 95/46/EC sur la protection des données

Le droit de l'Union se divise en traités et en droit dérivé. Depuis 1995, la directive 95/46/EC 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 est le principal acte juridique de l'UE sur la protection des données, et un des seuls instruments dont dispose actuellement la commission[30]. Elle avait été adoptée pour répondre à une double préoccupation. La première, était le retard du législateur européen, alors que plusieurs Etats-Membres avaient déjà adopté des lois nationales de protection des données. Il était en effet complexe d'assurer la libre circulation des marchandises, des capitaux, des services et des personnes dans le marché intérieur sans libre circulation des données, conditionnée par une véritable sécurisation des données avec la mise en place d'un haut niveau de protection. La deuxième, c'était la nécessité d'harmonisation du droit à laquelle répondait cette directive, pour assurer un niveau de protection comparable dans les 28 législations en vigueur[31]. La CJUE avait par ailleurs rappelé dans son arrêt 24 novembre 2011 sur les affaires jointes Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado que « *la directive 95/46 vise (...) à rendre équivalent dans tous les États membres le niveau de protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel* »[32]. Il y a donc une authentique volonté du législateur d'aller dans le sens d'une protection élevé du cadre juridique de la privacy pour sécuriser le marché intérieur. La directive 95/46/EC reprend les principes fondamentaux de la protection des données consacrées par la convention, mais elle

[30] Parlement Européen et Conseil, Directive 95/46/EC relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données

[31] Ibid considérants 1,4, 7, 8

[32] CJUE, Affaires Jointes Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado, 24 novembre 2011, points 28-29

y ajoute six critères pouvant légitimer le traitement des données[33]. Celui-ci n'est autorisé que si la personne concernée y a consenti expressément , ou si précisément son consentement est nécessaire à l'exécution d'un contrat auquel elle est partie, au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public, à la sauvegarde de son intérêt vitale ou à la protection de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévale pas l'intérêt de la personne concernée. La directive prévoit également la mise en place d'un réseau d'autorités de régulation dotées de missions et de compétences spéciales, qu'elles sont tenues « d'exercer en tout indépendance »[34], coopérant au sein du groupe du G29, au caractère consultatif et indépendant, actuellement présidé par la Présidente de la CNIL, Isabelle Falque-Pierrotin.

Cependant, cette directive manque de clarté sur plusieurs points, notamment sur la protection des utilisateurs quand à l'utilisation de leurs données par les entreprises ou les autorités de régulation des Etats-Tiers, ce qui entretient la confusion sur la question de savoir quel droit est applicable, et par qui ! Elle échoue également à stopper l'afflux des plaintes des entreprises quand à la diversité des procédures à travers les Etats-Membres. Dans le projet de règlement européen sur la protection des données 6 avril 2016, le Conseil de l'Union Européenne pointait d'une part « *l'insécurité juridique ou le sentiment, largement répandu dans le public, que des risques importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne »*[35], et d'autre part l'obstacle l'exercice des libertés économiques de l'Union, faussant la concurrence et empêchant les autorités de s'acquitter de leurs obligations découlant du droit de l'Union[36]. Par ailleurs, l'entrée en vigueur du traité de Lisbonne, en donnant une force juridique contraignante à la charte européenne des droits fondamentaux à consacré la nécessité d'élaborer un nouveau cadre juridique de la protection des données, s'appliquant dans l'ensemble des Etats-Membre[37]. L'enjeu visé aujourd'hui par le règlement européen sur la

[33] Directive 95/.46/EC article 2
[34] Ibid article 28 et 29
[35] Conseil de l'Union Européenne, Dossier inter-institutionnel du Règlement UE 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation des données, abrogeant la directive 95/46/EC, 6 avril 2016
[36] Ibid point 9
[37] Assemblée Nationale, Commission des Affaires Européenne, Rapport n°4326 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel au sein de l'UE, notamment dans le cadre de la réforme de la directive 94/46/CE, 7 février 2012

protection des données est donc une modification en profondeur de la législation existante, via l'harmonisation du droit primaire.

5. Le règlement européen d'avril 2016 : vers une harmonisation réelle de la protection de la donnée ?

L'article 16, paragraphe 2, du TFUE permet au Parlement européen et au Conseil de fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ainsi que les règles relatives à la libre circulation des données caractère personnel. Le paragraphe 1 de ce même article dispose en effet que « *Toute personne à droit à la protection de ses données personnelles* »[38]. Le règlement d'avril devant déboucher sur une directive en 2018, le Conseil de l'Union a rappelé sa volonté au point 10 du règlement de laisser aux Etats-Membres une marge de manœuvre concernant plusieurs législations sectorielles. De même, le Conseil rappelle dans ce même point que « *le traitement de données à caractère personnel nécessaire au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application des règles du présent règlement* »[39]. Il ouvre donc la voie à une série de justifications à des mesures contraires au droit de l'Union Européenne. En revanche, il reprend la directive 2000/31/CE du Parlement et du Conseil ayant pour objectif d'assurer la libre circulation des services de la société d'information entre les Etats Membres.

En décembre 2015, la Commission, le Conseil et le Parlement ont abouti à un accord politique sur le projet de règlement européen visant à améliorer la protection des données personnelles des citoyens. Le règlement européen, qui sera applicable en 2018, a pour objectif de remplacer les législations disparates des 28 Etats Membres dans le but de permettre à l'ensemble de l'Europe de s'adapter aux nouvelles réalités du numérique, par l'approfondissement du marché intérieur. Les Commission part en effet du postulat que seul un cadre un cadre solide et rigoureux de protection des données permettra à l'économie

[38] Traité sur le Fonctionnement de l'Union Européenne, article 16, paragraphe 1 et 2
[39] Ibid point 10

numérique de se développer dans l'ensemble du marché intérieur. En effet, bien que l'adoption de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données fut un acte fondateur de la protection de la vie privée à l'échelle communautaire, sa modernisation apparaît urgente, étant donné les différences de mise en œuvre entre les 28 Etats-Membres. Il apparaît cependant que les institutions européennes ont d'abord un objectif d'efficacité économique et d'amélioration de compétitivité des entreprises européennes. En effet par ce règlement, le législateur européen espère sécuriser la vente en ligne, et mettre en place les conditions d'une véritable croissance du e-commerce en Europe, avec une forte simplification des formalités administratives. Il est important de souligner la logique d'élaboration d'une « *doctrine européenne*[40] », de la protection des données par le biais d'un rapprochement des autorités de contrôle et de la mise en place d'un guichet unique. Le règlement CE n°45/2001 du Parlement Européen et du Conseil montre une volonté du législateur de s'en tenir à la réglementation de la protection des données en lien avec une activité professionnelle ou commerciale. Cependant, en opérant une distinction entre une telle activité et une activité personnelle et domestique, il ne donnait aucun détail quand aux moyens de séparer entre ces deux activités[41]. Or cette séparation est extrêmement difficile à opérer dans le cas d'un réseau social comme Facebook par exemple. Par ailleurs l'accord politique accorde une batterie d'exceptions aux Etats, reprenant la logique de la convention européenne des droits de l'homme de 1950. Cette série d'exceptions recouvre les mesures des Etats-Membres prises à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection et le préventions contre les menaces pour la sécurité publique, et enfin la libre circulation de ces données[42]. Cependant ce règlement, consacre deux droits fondamentaux pour les utilisateurs. Malgré les difficultés techniques d'invocation subsistantes et le manque de précision de ces deux droits, ils marquent une réelle volonté de la Commission Européenne d'améliorer les droits des citoyens européens. Le premier est consacré dans un article 17, c'est un principe qui avait été dégagé par le juge européen lors de l'affaire Google Spain de 2014 :

[40] CNIL, « Adoption du règlement européen par le Parlement Européen : un grand pas pour la protection des données en Europe » Article, 14 avril 2016

[41] Conseil de l'Union Européenne, Dossier inter-institutionnel du Règlement UE 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation des données, abrogeant la directive 95/46/EC, 6 avril 2016, Chapitre I, article 2

[42] Ibid

le droit à l'oubli et à l'effacement. La personne concernée aurait le droit d'obtenir l'effacement de données à caractère personnel et la cessation de la diffusion de ces données dans plusieurs cas. Par exemple, lorsqu'elles ne sont plus nécessaires pour les finalités prévues, lorsque la personne concernée retire son consentement, lorsqu'elle s'oppose au traitement à des fins de marketing, ou lorsque le traitement n'est pas conforme à la directive.[43] Cette textualisation du droit à l'oubli est une avancée considérable de la protection des droits fondamentaux des utilisateurs, malgré des faiblesses pointées par le législateur français dans son application. Par exemple, concernant les réseaux sociaux, la commission des affaires européennes de l'Assemblée Nationale a souligné dans un rapport la nécessité d'introduire une double protection en avançant d'une part l'effacement « *par principe* » des données d'un profil d'utilisateur après un certain délai sans usage, et d'autre part l'adoption d'un « *droit exprès et effectif à l'effacement de ses données et non pas à un simple droit de désactivation du profil* »[44]. En second lieu, le juge consacre à l'article 18 du règlement un droit à la portabilité des données, à savoir le droit pout la personne concernée d'obtenir une copie de ses données qui font l'objet d'un traitement, afin de pouvoir les réutiliser. C'est véritablement la consécration d'un droit de récupération de sa donnée ! Ce droit serait à la fois destiné à protéger le consommateur, et d'autre part à faciliter sa mobilité et celles des entreprises qui peuvent pleinement profiter des avantages du stockage de données par le Cloud Computing. Le législateur européen a donc centré le règlement adopté en avril sur l'allègement des charges administratives pour les entreprises, le rapprochement des autorités de contrôle, et la modernisation des droits des consommateurs. On étudiera dans une seconde partie l'influence considérable du juge européen sur la question des données, qui devance régulièrement le législateur sur les problématiques de la modernisation des droits, et la remise en question de l'américanisation du droit de l'Union Européenne provoquée par l'inflation de la cyber-surveillance.

[43] Ibid article 17

[44] Assemblée Nationale, Commission des Affaires Européenne, Rapport n°4326 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel au sein de l'UE, notamment dans le cadre de la réforme de la directive 94/46/CE

B. Les mutations du droit de l'Union: entre réglementation et autorégulation

1. Une harmonisation progressive marquée par de nouvelles libertés

L'avocat Sylvain Métille, enseignant à la faculté de droit de Lausanne, affirme que la question centrale de la protection des données est celle de la notification. Celle-ci, variable dans la forme et dans la durée selon l'Etat Membre dans lequel on se trouve, avertit l'utilisateur du traitement de ses données, en général par une page proposant une option « *accepter* » et une option « *refuser* ». Le problème c'est que suivant ce mécanisme, une banque peut refuser un crédit à un particulier, celui-ci ayant accepté une analyse financière de sa situation pour acheter un abonnement quelconque deux ans plus tôt. Au delà de l'acceptation, le particulier se voit protégé par deux droits. Le premier que nous aborderons brièvement est le droit d'auteur. Imaginons un instant que des photos qui appartiennent à un citoyen européen, soient réutilisées dans un magazine publicitaire après qu'il ait notifié au-dit magazine « j'accepte ». Le magazine n'a le droit d'utiliser ces photos seulement que si le droit d'auteur a été cédé valablement. On touche ici à la base juridique du « droit à l'image des personnes », qui trouve son fondement dans l'article 9 du code civil. Cet article dispose que « *chacun a droit au respect de sa vie privé, Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.* »[45]. Par conséquent, dès lors qu'une personne est le sujet principal de l'image et est parfaitement reconnaissable, il faut obtenir son autorisation. On est face ici à un arbitrage permanent que doit effectuer le juge entre la liberté artistique et le droit à l'image. La CEDH a une interprétation très rigoureuse en la matière qu'on retrouve dans l'arrêt Vereinibung Bildender Kunstler contre Autriche, rendu le 25 janvier 2007[46]. L'artiste Otto Mühl avait exposé en juin 1998 une peinture intitulée « Apocalypse », et présentée au public lors d'une exposition organisée en juin 1998 par

[45] Code Civil, Livre I, Titre I « Des droits civils », article 9
[46] Cour Européenne des Droits de l'Homme, Vereinigung Bildender Künstler c. Autriche, 25 janvier 2007

l'association requérante[47]. Elle montrait un ancien secrétaire général du Parti libéral autrichien (FPÖ) dans une position pour le moins dégradante, impliquant une représentation de Mère Teresa. La peinture fut interdite d'exposition, et l'association requérante condamnée à une amende. La cour souligna ici que « *la satire est une forme d'expression artistique et de commentaire social qui, par son degré d'exagération et de distorsion de la réalité inhérent à ses caractéristiques, vise, naturellement, à provoquer et à heurter* »[48], et se concentra sur l'arbitrage qui nous intéresse, entre la liberté d'expression artistique et la protection des droits d'autrui. Or, la CEDH considéra que la nature des fonctions de l'homme politique en tant que personne publique ne justifiait pas une telle interdiction, et conclut à la violation de l'article 10. Elle reprend ainsi la position du juge Spielmann dans l'arrêt fondateur Muller contre Suisse de 1988[49]. Le second grand volet, c'est le sujet de la protection des données. On protège l'identité de la personne, sa « personnalité ». Si celle-ci est atteinte, le particulier peut retirer son consentement. Cependant, l'universitaire américain Lawrence Lessig conteste cette vision « sacralisé » du travail de l'artiste. Estimant qu'on « *n'a jamais contrôlé à ce point l'usage de la culture qui nous entoure »* et que *« c'est une vision extrême du copyright qui conduit nos enfants à braver la prohibition* »[50], il plaide pour la mise en place d'un forfait culturel conditionnant l'accès aux œuvres sur Internet. Partisan de la contractualisation, il estime que celle-ci ouvre à l'utilisateur un véritable droit d'utilisation de sa donnée.

L'idée d'un droit à l'oubli ne date pas d'hier. La doctrine juridique française la rattache à la défense de l'intérêt public, par exemple lors de l'application du principe de prescription. La puissance publique souhaite finalement imposer le silence sur les fautes des citoyens dans certains cas, pour garantir paix et cohésion sociale. Selon Yves Poullet, directeur du centre de recherches informatiques et droit (CRID), la montée en puissance du numérique change profondément les aboutissants de ce droit. Il déclare en effet que "*Pour la première fois quasiment, on s'intéresse légalement à ce qu'il y a entre l'individu et celui qui traite ses données : l'outil technologique et ses potentialités.*"[51] La France en 1975, avait initié ce mouvement vers le droit à l'oubli en empêchant la préservation de bases de données pour les

[47] Ibid p4
[48] Ibid p10, point 33
[49] Cour Européenne des Droits de l'Homme, arrêt Muller contre Suisse, 24 mai 1988
[50] Lausson, Julien « *Lawrence Lessig : couper l'accès à Internet, une idée terrible* » Numerama 21 novembre 2009
[51] Dumontel, Fabienne « *Le droit à l'oubli numérique inquiète les historiens* », Le Monde, 3 octobre 2013

personnes interdites de chéquier après un laps de temps donné. A l'instar de 13 de nos voisins européens, la CNIL appelle depuis 2009 à une inscription du droit à l'oubli numérique dans la constitution, en adoptant un raisonnement semblable à celui de la charte de l'écologie. Le tribunal constitutionnel fédéral allemand avait aussi reconnu en 1983 un droit à « *l'autodétermination informationnelle* »[52]. En l'espèce, l'Allemagne avait dépassé le cadre du droit à être oublié, en donnant à ses citoyens la clé d'une réelle maîtrise de leurs informations personnelles pour créer les conditions d'un environnement numérique sûr et transparent. C'est cet objectif qui est visé par l'Union Européenne, aussi bien par le règlement européen de la Commission que par la jurisprudence plus hésitante et moins ambitieuse de la Cour. Le 13 mai 2015, la CJUE a rendu un arrêt consacrant la naissance d'un véritable droit à l'oubli dans l'affaire Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González[53]. En l'espèce, le citoyen espagnol Costeja Gonzales avait envoyé une plainte à l'autorité de protection des données espagnoles, la *Agencia Española de Protección de Datos* à l'encontre d'un éditeur de presse en ligne appelé "La Vanguardia", et les sociétés Google Spain et Google Inc. Si un utilisateur effectuait une recherche avec son nom, les résultats renvoyaient un à un à un quotidien traitant d'une vente aux enchères immobilières effectuée à la suite d'une saisie pratiquée en recouvrement des dettes sociales de Monsieur Costeja. Or ces informations n'étaient plus pertinentes, puisque cette procédure avais été clôturée, et le requérant s'estimait lésé par cet article portant atteinte à la protection de ses données personnelles. A la suite d'un premier refus de Google Spain et Google Inc, l'agence de protection des données espagnoles a accueilli favorablement la réclamation de Monsieur Costeja, estimant qu'elle était compétente pour ordonner le retrait des données et l'interdiction d'accéder à certaines données par les exploitants de moteurs de recherche «lorsqu'elle considère que *« leur localisation et leur diffusion sont susceptibles de porter atteinte au droit fondamental de protection des données et à la dignité des personnes au sens large, ce qui engloberait également la simple volonté de la personne intéressée que ces données ne soient pas connues par des tiers* ».[54]. A la suite de cette décision, les sociétés Google Spain et Google Inc ont ont alors introduit deux recours séparés devant la CJUE. L'argument de la multinationale étant le suivant : quelles obligations incombent aux

[52] Poullet, Yves, et Rouvroy, Antoinette «*Le droit à l'auto-détermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie* », Article de monographie, 2009, p1

[53] CJUE Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, affaire C-131/12, 13 mai 2015

[54] Ibid point 17

exploitants de moteurs de recherche, dans un contexte d'émergence de nouvelles technologies apparues après la publication de la directive 95/46/CE ? Elle argue également que « *l'activité des moteurs de recherche ne saurait être considérée comme un traitement des données qui apparaissent sur les pages web de tiers affichées dans la liste des résultats de la recherche, étant donné que ces moteurs traitent les informations accessibles sur Internet dans leur ensemble sans faire le tri entre les données à caractère personnel et les autres informations* »[55]. Ici, on touche au point nodal de la positon de la CJUE, qui tend à s'ériger en Cour des droits fondamentaux. Elle avait déjà affirmé dans un arrêt Lindqvist en 2003 que l'opération qui consiste à faire apparaître sur une page Internet des données à caractère personnel est à considérer comme un « *traitement des données à caractère personnel* » au sens de la directive de 1998[56]. Elle avait également constaté en 2008 dans un arrêt Satakunnan Markkinapörssi et Satamedia [57]que les opérations visées à l'article 2,b de la directive devaient être qualifiées comme un tel traitement, lorsqu'elles concernent des hypothèses déjà publiées telles quelles dans les médias. L'arrêt qui nous occupe n'est donc que la traduction juridique d'une volonté de protection du « e-citoyen » qui ne date pas d'hier. Dans le présent arrêt, la Cour rappelle tout d'abord dans son raisonnement le cadre juridique d'une telle problématique : les activités de moteurs de recherche sont des « traitement de données à caractère personnel » au sens de la directive 95/46/CE. La Commission montre également que l'exploitant d'un moteur de recherche serait *« responsable du traitement des données effectué par celui-ci dès lors que c'est lui qui détermine les finalités et les moyens de ce traitement ».* La conséquence de ce constat, c'est que si les dispositions de la directive s'appliquent aux moteurs de recherche, la cour en déduit qu'ils sont tenus de respecter les droits d'accès et d'opposition prévus par la directive, à l'article 14 : *« Les États membres reconnaissent à la personne concernée le droit de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données »*[58]. Il va sans dire que l'entreprise et les moteurs de recherches furent contrariés

[55] Ibid point 22
[56] CJUE Bodil Lindqvist, affaire C-101/01 6 novembre 2003
[57] CJUE Satakunnan Markkinapörssi et Satamedia, affaire C-73/07, 16 décembre 2008
[58] Parlement Européen et Conseil, Directive 95/46/EC relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, article 14

par cette décision, les représentants de Google manifestant leur surprise devant un arrêt s'éloignant autant des conclusions et des recommandations de l'avocat général. C'est véritablement l'ouverture d'un droit pour la personne concernée à demander l'arrêt de l'affichage de certaines de ses données sur Internet, par le biais de la suppression d'un ou plusieurs résultats. Un tel système implique plusieurs choses : d'abord la recherche d'un équilibre entre ce droit à l'oubli et la liberté d'expression et le droit à l'information. La deuxième chose, c'est la délégation à Google du soin de trouver une solution concrète pour appliquer ce droit, ce que l'entreprise a fait en mettant en place un formulaire permettant aux internautes de demander la suppression de leurs résultats. Il y a ici un véritable paradoxe, puisque d'un côté la cour s'érige en gardienne des droits fondamentaux des citoyens, et de l'autre, elle laisse au moteur de recherche la liberté d'appliquer sa propre condamnation, sans contrôle sur la mise en œuvre du droit au déférencement. Cet arrêt révèle deux éléments préoccupants. D'une part, la cour est la seule à monter au fronton pour défendre les données des citoyens, de façon beaucoup plus efficace que la Commission qui suit la volonté des états. La seconde chose, c'est l'ignorance absolue du législateur comme du juge de solutions techniques à même de résoudre les problématiques du numérique, jusqu'à déléguer aux plateformes le soin de la solution du droit à l'oubli ! On touche ici aux limites du droit, et donc à celles des capacités de la Cour, bornée par son ignorance relative en matière d'informatique.

Le juge américain James Rosenbaum pointe dans son ouvrage « In defense of the DELETE key » le fait que les ordinateurs n'oublient rien, et dénonce la possibilité pour la justice de se saisir de documents virtuellement détruits pour accuser leur auteur. Il argue qu'une société est plus libre et moins en danger lorsque *« le faux, le vénal, le potentiellement mauvais est exprimé au grand jour sur la place de « marché des idées » »*[59]. Le droit de changer d'opinion et de chemin de vie participe aussi au respect de la vie privé. Sur une autre question, celle du principe d'extraterritorialité, qui s'oppose en pratique à l'application d'une législation nationale à l'encontre d'un acteur de l'Internet situé à l'étranger, un rapport d'information de 2008 rédigé par le député Français Patrick Verchère pointait les stratégies individuelles d'entreprises telles que Google pour développer leurs propres règles en l'absence de réglementations précises leur étant applicables. Parallèlement à une véritable délégation de la protection des données, ou de leur effacement au secteur privé, le manque

[59] Rosenbaumn, James « *In defense of the delete key »* The Green Bag, été 2000

d'harmonisation laisse aux acteurs de la toile une marge de manœuvre considérable. A titre d'exemple, le député constatait dans son rapport que Google possèdait une technologie permettant de bloquer sur un territoire donné un contenu jugé illicite, tout en maintenant son accessibilité ailleurs. Or, pour que la législation d'un Etat-Membre puisse s'appliquer à Google, celle-ci doit cumuler deux critères : l'existence d'une filiale de la société dans le pays concerné, et celle d'une activité de promotion commerciale dans la société[60]. Or en l'absence de ce cumul, le rapport dénonce le fait que la société Google ne « *tient pas compte des législations des pays où elle n'est pas implantée. Cette position peut alors être source de tensions avec les pays concernés, dans la mesure où les services de Google y sont tout de même accessibles* ». [61] Malgré les avancées considérables du législateur européen dans le règlement voté en avril, notamment sur des questions comme celles du droit à l'oubli, à la portabilité, et au renforcement du consentement et de l'information des personnes, ce règlement souffre d'insuffisances profondes. En effet dans un contexte international où la surveillance du consommateur par les Etats et les entreprises devient la norme, l'édifice juridique patiemment bâti par les institutions de l'Union Européenne et le Conseil de l'Europe apparait aujourd'hui bien fragile.

2. La neutralité du net remise en question par les enjeux de cyber surveillance

Evoquer les enjeux de régulation entourant le phénomène de la donnée, c'est penser directement à la protection des données de nos concitoyens à l'heure où l'arme la plus puissante dont dispose les gouvernants est la détention de l'information. Aux Etats-Unis avec le programme PRISM mis en place après les attentats du 11 septembre 2011, ou la loi de programmation militaire en France entérinée par le sénat le 18 décembre 2013, autorisent la surveillance des citoyens sur les réseaux informatiques, sans passer par le contrôle de la justice. Ainsi, entre le 10 décembre 2012 et le 8 janvier 2013, les services secrets américains auraient effectué 70,3 millions d'enregistrements de données téléphoniques des Français, avec

[60] Assemblée Nationale, Rapport d'information n°3560 de M. Patrice Verchère, « Révolution numérique et droits de l'individu : pour un citoyen libre et informé » 22 juin 2011, p184
[61] Ibid

des pics avoisinant les 7 millions d'enregistrements par jour.[62] Révélé au monde par le consultant américain Edward Snowden, ce phénomène ciblait non seulement les données, mais aussi les conversations de certains citoyens, les logiciels de la NSA enregistrant automatiquement certains échanges à partir d'une alerte. Mais ce gigantesque phénomène de surveillance ne se limitait pas aux Etats-Unis, il s'étendait à ce que certains journaux ont nommés les « five eyes ». En Allemagne, la NSA aurait capté sur la période du 24 décembre 2012 au 7 janvier 2013 la modique quantité de 10 et 20 millions de données de connexion téléphonique par jour, avec un maximum de 49 millions le 7 janvier[63]. A l'époque, les institutions européennes s'étaient également trouvé en ligne de mire de la NSA, qui d'après le journal allemand Spiegel avait plaçé des micros dans les ambassades et les missions diplomatiques de l'Union Européenne à Washington et à New York. Ces révélations avaient provoqué une réaction inquiète de Martin Schultz, qui s'était déclaré « *profondément inquiet et choqué par les allégations d'espionnage des autorités américaines dans les bureaux de l'UE* ». Il avait également déploré les conséquences nuisibles de ces révelations sur les relations entre l'Union Européenne et les Etats-Unis et avait réclamé « *une pleine clarification et des informations complémentaires rapides* » de la part des de l'administration américaine.[64] Cette surveillance exercée par les Etats-Unis trouve son origine dans le programme PRISM, qui a vu le jour suite à la signature du Protect America Act en 2007 par le président Georges W Bush. Cet amendement retirait l'obligation d'une autorisation des tribunaux avant de lancer des programmes de surveillance à l'étranger. Pour le citer, le directeur de la NSA de l'époque, J. Michael Mc Connell, avait déclaré devant le congrès que « *the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States"*. Il avait par ailleurs justifier cette mesure part la nécessité d'une plus grande souplesse et de moyens d'actions rapides pour les agences de surveillance américaine pour mener à bien leur guerre contre le terrorisme. Démontrant que *"This provision is at the heart of this legislation"* il avait montré que cette mesure ne pouvait être efficace que si la NSA n'avait

---

[62] Kallenborn, Gilbert « *La France a été la cible d'une cyber surveillance massive par la NSA* », Journal 01.net, 1er juillet 2013

[63] Ibid
[64] Ibid

plus à obtenir l'approbation de la cour si la cible était située en degors des Etats-Unis[65]. Le deuxième instrument juridique permettant ce type d'opération, c'est le FISA Amendements Act de 2008, qui donne aux entreprises assistant le gouvernement américain dans leur collecte des données une immunité légale. Ce dernier a été renouvelé par Barack Obama pour une période de 5 ans en décembre 2012, et autorise le gouvernement des Etats-Unis à surveiller les communications électroniques. L'article 702 de cette loi permet au Procureur Général des Etats-Unis et au Directeur du renseignement national d'autoriser ensemble l'acquisition de données pendant un an. Les législateurs américains ont par ailleurs borné l'utilisation de cet instrument par certaines conditions à l'article 702, notamment l'approbation d'un juge « *the Foreign Intelligence Surveillance Court must approve the targeting and minimization procedures, which helps ensure the protection of privacy and civil liberties.* », et la destruction des données récoltées lorsqu'elles ne rentrent pas dans le champ d'application : « *any information collected after a foreign target enters the U.S. –or prior to a discovery that any target erroneously believed to be foreign was in fact a U.S. person– must be promptly destroyed unless that information meets specific, limited criteria approved by the Foreign Intelligence Surveillance Court.* »[66]. Il est également indiqué que la collecte des données doit être menée en compatibilité avec le quatrième amendement de la constitution américaine qui protège des perquisitions et saisies non motivées, une possibilité déjà limité puisque cette loi vise majoritairement à récolter les données d'étrangers sur un sol étranger. Cependant rien n'empêche la collecte « accidentelle » des messages, emails, textos, et vidéos d'américains, d'autant plus si ils entretiennent une communication électronique avec un étranger en dehors du territoire[67]. La Section 702 du FISA autorise par conséquent la mise en place de programmes de surveillances élaborés par la NSA, dont le fameux programme PRISM ayant provoqué les révélations d'Edward Snowden. Le schéma présenté en page 41, élaboré par le Washington Post, illustre très bien l'impact et le fonctionnement d'un tel système, centré sur l'organisation d'une cyber-surveillance en collaboration avec le secteur privé. Le premier géant du numérique à y participer fut l'entreprise Microsoft en 2007, suivie de Yahoo en

[65]US Senate, Juciary Committee, September 18, 2007 Statement for the Record to the House Judiciary Committee by Director John Michael McConnell

[66] US Senate, Foreign Intelligence Service Act (FISA), Title VII, Section 702 Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons"

[67] Gellman, Barton, et Lindeman, Todd, « *Inner workings of a top-secret spy program* », The Washington Post, 1er juin 2013

2008, de Google, Paltak et Facebook en 2009, de Youtube en 2010, de AOL et Skype en 2011, et de Apple en 2012. [68] Or l'ensemble de ces firmes a nié avoir participé à la collecte illégale de données de leurs utilisateurs dans une série de déclarations suivants les révélations de Snowden. Les représentants de Google avaient alors déclarés à la presse « *Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a back door for the government to access private user data.*"[69]. Ceux de Facebook avaient rappelés l'attachement de l'entreprise à la sécurité des données de ses utilisateurs, avant d'expliquer leur mode de fonctionnement face à ce type de programme : « *When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law* »[70]. Quand à l'entreprise Microsoft, elle avait fermement démentie sa participation à un tel programme : « *We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data, we don't participate in it.* » [71] Ces déclarations nous amènent à une véritable interrogation sur deux phénomènes. En premier lieu, la part de responsabilité des géants du numérique dans la violation manifeste des droits des citoyens américains, et par extension de ceux des européens. D'autre part, elles nous amènent à une véritable interrogation sur la meilleure manière de contrôler les programmes de surveillance, qui au nom de la lutte contre le terrorisme, voient les agences de renseignement américaines échapper au contrôle de la justice. Le 23 octobre 2013, le Parlement Européen a adopté une résolution suspendant l'accord SWIFT, rappelant que « *les mesures de sécurité doivent s'inscrire dans l'état de droit et être subordonnées aux obligations en matière de droits fondamentaux, y compris celles qui ont trait à la vie privée et à la protection des données* »[72]. La dite résolution a donc torpillé le traité international TFTP dit SWIFT II qui permettait depuis le 1er août 2010 à l'administration gouvernementale des

[68] Kevin Johnson, Scott Martin, Jayne O'Donnell and Michael Winter, « *Reports: NSA Siphons Data from 9 Major Net Firms".* USA Today. 15 juin 2013
[69] Ibid
[70]Ibid
[71] Ibid
[72] Parlement Européen, Résolution sur la suspension de l'accord TFTP du fait de la surveillance exercée par l'agence nationale de sécurité américaine. 23 octobre 2013

Etats-Unis d'avoir accès aux données des banques européennes pour lutter contre le terrorisme. La banque américaine de droit belge Society for Worlwide Interbank Communication (SWIFT) établie près de Bruxelles avait en effet été soumise aux injonctions répétées du ministère américain de fournir des données confidentielles sur certains de ses clients pour soutenir la lutte contre le terrorisme, en violation totale des dispositions de la directive 95/46/CE et de l'article 8 de la Charte des droits fondamentaux. La directive dispose en effet que ces données personnelles concernent « *toute information concernant une personne physique identifiée ou identifiable* », et « *qu'une personne peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* »[73]. Or en l'espèce, la société SWIFT avait transmis à l'administration américaine des données faisant mention de l'identité de plusieurs de leurs propriétaires. Le G29 a par ailleurs rendu en avis mettant en cause le violation des règles européennes de protection des données par la société, qui était rentré dans l'illégalité en« *acceptant de communiquer aux autorités américaines des données transitant par son réseau*» [74]. Si la Commission de la protection de la vie privé belge accepta de clore les poursuites judiciaires engagées contre SWITF après deux ans d'enquête, les institutions se saisirent du problème et l'accord SWIFT I fut signé 30 novembre 2009 par 29 gouvernements. En fin de compte, il fut rejeté par la Commission des Libertés Civiles et des Libertés du Parlement Européen, profitant du droit de regard sur les traités internationaux négociés dans les domaines de la coopération judiciaire et policière qui lui avait été accordé par le Traité de Lisbonne[75]. Ce rejet est révélateur de la difficulté considérable à opérer un arbitrage entre l'impératif de sécurité et celui de liberté, mais aussi de l'émergence progressive de l'institution parlementaire sur ces problématiques, faisant office de garde fou des droits fondamentaux des citoyens européens.

---

[73] Parlement Européen, , Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. 24 octobre 1995

[74] CNIL, 5 décembre 2006, « *Le G29 confirme que SWIFT a violé les règles européennes de protection des données* »

[75] Letschert, Iris « *Les accords SWIFT : un nouveau pas dans la collaboration internationale de lutte contre le terrorisme au détriment du droit européen de la protection des données à caractère personnel* ? » article publié sur le blog de l'Université Paris X Nanterre, 15 février 2010

Le schéma de la page 41 illustre les différentes étapes du programme de surveillance « Terrorism Finance Tracking program ». Il me paraît important de montrer au lecteur le fonctionnement d'un tel programme : un analyste de la NSA va entrer dans la barre de recherche du programme un ou plusieurs termes, appelés des « selectors » pouvant être des informations diverses sur la personne concernée: nom, adresse e-mail, numéro de téléphone, signature numérique etc[76]. Après cela, l'analyste doit justifier sa recherche par une éventuelle menace à la défense nationale, puis s'assurer que celle-ci ne mènera pas à un citoyen des Etats-Unis ou à un résident sur le territoire américain. Par la suite, la demande de recherche entrée dans le programme, qu'on appelle « tasking », est envoyée à différentes sources, notamment les entreprises privées, les « PRISM providers » ayant acceptées de participer au programme, qui peuvent traiter la demande en fonction du domaine dans lequel elles sont spécialisées : Youtube pourra fournir des données vidéos, Yahoo des emails etc. Les communications électroniques collectées par la NSA recouvrent 11 types différents, répertoriés ci-contre : des photos, des informations extraites du Cloud computing, des vidéos, des messages, transporteurs de fichiers, des communications issues des réseaux sociaux… Une fois la demande transmise, l'ensemble des données sur la cible sont transférées dans un système complexe mis en place par la NSA appelé le programme PRINTAURA, illustré sur l'image par un cerveau encastré dans une boîte de verre[77]. Au cours de cette procédure, la NSA vérifie à une seconde reprise que la donnée ne concerne pas un citoyen américain ou une personne résident sur le territoire des Etats-Unis, puis elle transmet automatiquement les données à l'analyste de la NSA, ce qui peut prendre plusieurs heures. Cette surveillance ne se limite pas au Programme PRISM, et s'étend à bien d'autres programmes tel que le système UPSTREAM, qui avait permis à la NSA d'utiliser les réseaux téléphoniques pour les mettre sur écoute. Ce programme de surveillance, exemple flagrant de la perception anglo-saxonne de la protection de la vie privé, n'est qu'un des nombreux canaux de collecte des données. En effet aux Etats-Unis, des sociétés comme PublicData.com proposent un accès à des bases de données administratives sur des citoyens européens moyennant un abonnement mensuel de 30 euros[78]. Choicepoint, une autre société, à passé un contrat avec avec l'administration fiscale et le FBI pour que ceux-ci connaître des données aussi personnelles

[76] [76] Gellman Barton et Lindeman Todd, « *Inner workings of a top-secret spy program* », The Washington Post, 1er juin 2013

[77] Ibid

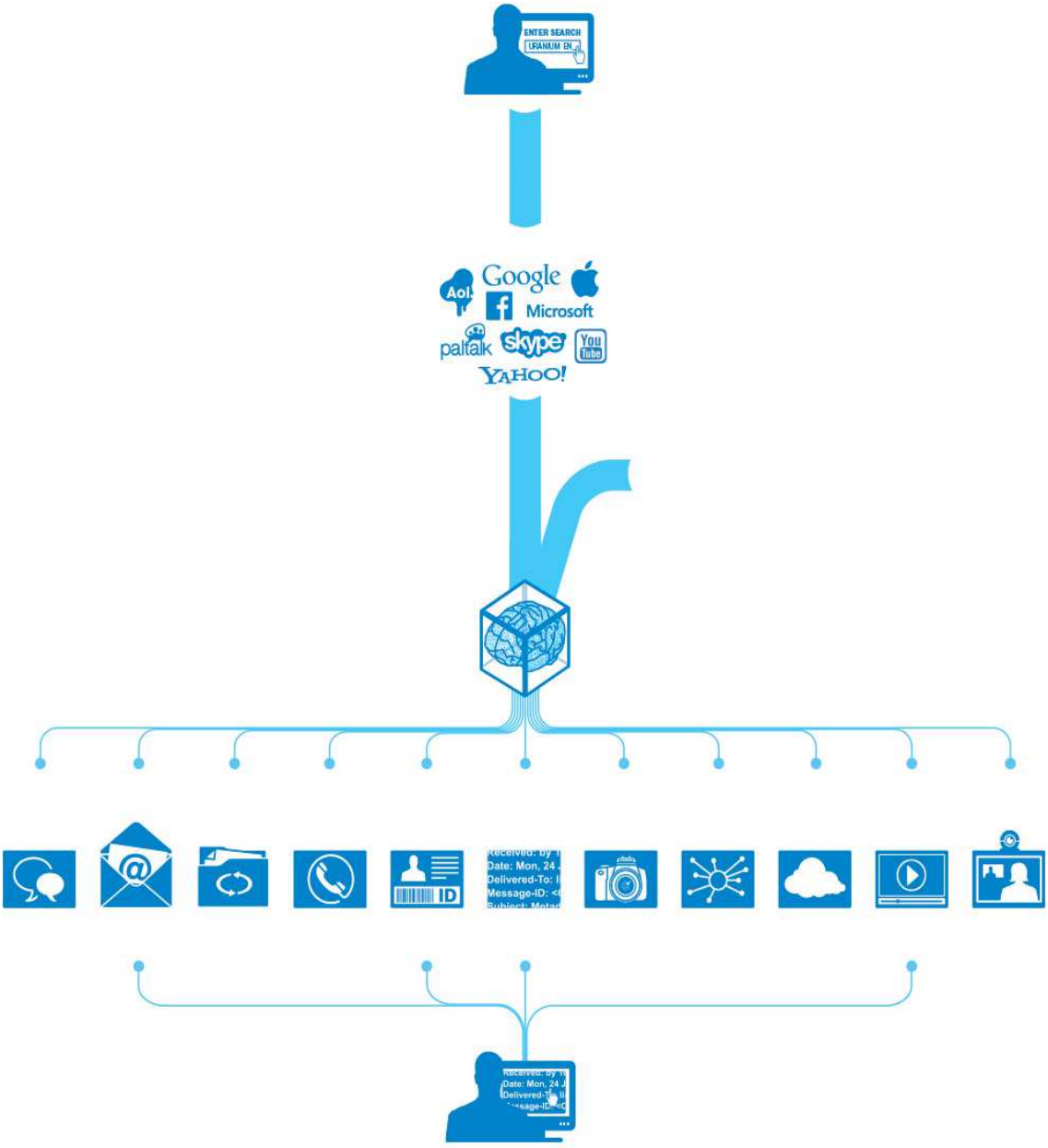
[78] p128

que la valeur du patrimoine des contribuables, leurs infractions au code de la route, leur numéro de téléphone privé. En tout ce sont 10 milliards d'informations personnelles qui sont proposées par cette entreprise, et classées en fonction des numéros de sécurité sociale de chaque américain [79] . Dans la sphère professionnelle, les trois quarts des entreprises américaines opèrent une surveillance constante sur les communications de leurs salariés[80]. Le consommateur, séduit par la gratuité qui caractérise l'utilisation d'Internet, en oublie souvent la contrepartie. Face à une telle industrialisation de la collecte des données, on peut s'interroger sur l'intervention étatique la plus adaptée pour canaliser la recherche d'informations et leur utilisation.

[79] Boulet-Gercourt, Philippe « *Votre vie les intéresse* » Le Nouvel Observateur, 26 juillet 2001

[80] Godeluck, Solveig « *La géopolitique d'Internet* » La Découverte, 2002 p 134

Fonctionnement du Programme PRISM : [81]



[81] Gellman Barton et Lindeman Todd, « *Inner workings of a top-secret spy program* », The Washington Post, 1er juin 2013

C. La régulation d'internet, une approche fondée sur la gestion du bien commun

1. L'économie des communs, une approche gestionnaire d'Internet

Une théorie originale de gestion du bien commun de l'internet a vu le jour dans les années 1990. Elle justifie aujourd'hui des déclarations qui nous sont aussi familières que « Ceux qui n'ont rien fait de mal n'ont rien à cacher ». Discours typique, révélant l'inertie des sociétés démocratiques face à la surveillance, puisqu'elle n'est pas du fait d'un Etat Léviathan mais d'une multitude d'acteurs économiques désunis. C'est la grande vague de la propriété privé des données personnelles et des « infomédiaires », identifiés par les américains John Hagel et Marc Signer en 1999[82]. Ces fameux infomédiaires seraient chargés de la protection du client, et négocieraient directement avec lui la confidentialité de ses données personnelles et la vente de certaines d'entre elles à des sociétés commerciales. Cette vague s'est traduite par la création des « Privacy enhancing technologies », des technologies de renforcement de la vie privé, permettant à l'utilisateur d'avoir une réelle maîtrise sur ses données. Ces dispositifs peuvent être décrits comme un système de mesures protégeant les données personnelles, en prévenant l'utilisateur d'un usage de ses données qui serait superflue ou non souhaité. On assiste ici à l'émergence d'un phénomène de contractualisation entre ces logiciels privés et les utilisateurs. La mise en place de la plateforme des préférence des données par le biais du logiciel P3P avais été prévu à cet effet : un utilisateur pouvait, grâce à ce standard élaboré par le « World Wide Web consortium » (une organisation internationale élaborant des standards techniques pour Internet) bannir les sites dont il n'acceptait pas les conditions. Cette solution est doublement avantageuse, puisqu'elle crée un levier de contrôle des données accessible à l'internaute, et incite les entreprises à une réelle transparence sur leur politique de protection de la vie privé. Lawrence Lessig, professeur de droit à l'université de Harvard et fondateur du « Center for Internet and Society », plaide pour le vote d'une loi créant un droit de propriété sur la vie privé instituant ainsi une reconnaissance du « bien

[82]Mousil, Marc « *Valeur sur le Net. Infomédiaires: les nouveaux champions du Web John Hagel et Marc Singer* » Alternatives Economiques n°185, Octobre 2000

commun » Internet. Cette vision américaine est un véritable pendant numérique des thèses Coasienne sur les marchés des droits à polluer. Elle est en cohérence avec l'idéologie libérale consistant à privilégier la mise en place de dispositifs d'autorégulation à une réglementation stricte, pouvant instaurer un régime de responsabilité civile. Ce même professeur justifie ce choix par l'existence d'une négociation précédant la vente de données, conditionnant cette vente à une demande de la part de celui qui veut profiter de la ressource. Fervent partisan de l'autorégulation, il estime qu'à la naissance d'Internet, celui-ci offrait aux individus un plus haut degré de liberté d'expression et de protection de la vie privé, et pouvait être considéré comme un véritable bien commun, les Etats ne disposant pas à l'époque des instruments nécessaires à la cyber-surveillance[83]. On en vient à réfléchir sur la nature des leviers qu'on souhaite confier aux citoyens. Est-il pertinent d'encourager la création de marchés de la donnée, et la considération de ces éléments de l'identité citoyenne comme « *le nouveau pétrole de l'économie* » ? La mise en place d'une propriété privée des données reviendrait à remettre en cause le régime de protection des données, construit pour dissuader l'utilisateur de publier ses informations, non pour l'encourager à en faire commerce.[84] Le juriste Marc Rotenberg s'oppose vivement à l'approche libérale de Lessig sur la donnée, estimant que « *le droit à la vie privé n'est pas une propriété mais une valeur politique* ». Dans un contexte de collecte de la donnée, et de violation permanente des régimes de protection souvent inefficaces, une contractualisation de la donnée ferait basculer les utilisateurs du monde entier de la privacy, donc du droit à ne pas être publié, au copyright, protégeant un intérêt après sa publication[85].

Aujourd'hui, on peut légitimement s'interroger sur la nature du vecteur des communications électroniques, Internet, comme un bien commun, dépassant la séparation traditionnelle entre bien privé et bien public. Les noms de domaines, sans lesquels d'après le Professeur Georges Chatillon, Internet serait « *une invention définissant un non espace de communication* »[86], ne sont pas des biens privés, puisqu'on on ne peut pas leur appliquer le droit de la propriété intellectuelle, mais ce ne sont pas pour autant des biens publics,

[83] Lessign Lawrence « *L'avenir des idées : le sort des biens communs à l'heure du numérique* » Broché, 1er septembre 2005, p174
[84] Rotenberg, Marc « *Fair informations practices and the architecture of privacy* » Stanford Technologiy Law Revew, 2001
[85] Ibid
[86] Chatillon, Georges « *L'internet : bien public-bien privé-bien commun* » annuaire de le l'Université Paris I Panthéon Sorbonne

puisqu'un utilisateur doit payer pour bénéficier d'une jouissance exclusive du nom de domaine. De plus, en effet si une marque est un titre de propriété délivré par une administration nationale d'une validité de 10 ans, un nom de domaine n'est qu'un enregistrement contractuel valable pour une durée de 1 an obtenu auprès d'une société privé ayant obtenu un agrément, directement ou indirectement, de la société de droit californien ICANN [87] , sur laquelle nous reviendront. En réponse à une question prioritaire de constitutionnalité, le Conseil Constitutionnel avait reconnu le nature hybride du droit des noms de domaines en 2010 dans une décision n°2010-45 : *« pour ceux qui exercent leur activité en ligne, l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte les droits de la propriété intellectuelle, la liberté de communication, et la liberté d'entreprendre* [88]». Véritable pilier d'internet, le nom de domaine et son bon fonctionnement conditionne en effet l'ensemble des activités en ligne. Le danger vient donc nécessairement de l'appropriation par les états souverains de ce bien commun, formé par l'espace entre deux noms de domaines. En effet, dans les limites de leurs frontières physiques, les états ont le droit de règlementer cet espace de communications électronique. Or les conventions internationales sur les télécommunications restreignent fortement la possibilité pour les états de couper une interconnexion sans qu'une telle mesure soit motivée par une décision d'une cour de justice ou par le droit international, et interdisent de collecter une catégorie de noms de domaines en les rendant inaccessibles à la communauté d'utlisateurs[89]. Malgré ces restrictions, le blocage des noms de domaines est une pratique courante de nombreux états, et cela malgré la hausse fulgurante des enregistrements de noms de domaines, avec au mois de mai 2015 presque 300 millions de dépôts, dont 40% de part de marché pour .com. Pour gérer une telle inflation, on étudiera ensuite le fonctionnement de la gouvernance d'Internet.

[87] Manara, Cedric « *Le noms de domaines : fondation du droit de l'internet* » Power point sur le livre « *Les droit des noms de domaines* », 13 avril 2012
[88] Conseil Constitutionnel, Décision n°2010-45, QPC du 6 octobre 2010, point 5
[89] Chatillon, Georges « *L'internet : bien public-bien privé-bien commun* » annuaire de le l'Université Paris I Panthéon Sorbonne

2. La gouvernance d'Internet

Pour comprendre l'élaboration progressive par nos législateurs d'un régime de protection des citoyens de l'Union Européenne, il est essentiel d'analyser la particularité de la gouvernance d'Internet et de la production de normes encadrant son utilisation, selon des modèles extrêmement variables. Pierre Trudel, professeur au centre de recherche en droit public de l'Université de Montréal, a montré que ce qui faisait la spécificité d'Internet, c'est la remise en cause profonde de nos modèles traditionnels axés sur l'application du droit e à une communauté bien définie. En effet l'émergence de puissantes communautés d'usagers aux « intérêts, langues, goûts et prédilections » en communs remplacent progressivement les communautés nationales classiques, par ce qu'il appelle un « droit du cyberespace »[90]. Il est donc nécessaire pour les législateurs de redéfinir les règles du jeu autour de cette évolution de la nature des communautés. De la même manière, Hans Klein, auteur de "La gouvernance d'Internet" [91], pointe la particularité de ce phénomène, véritable "*royaume d'anarchie bienveillante*". En effet, la régulation d'Internet est extrêmement complexe : l'anonymat des internautes, le fragile équilibre entre protection des droits et libertés économiques, les enjeux de cyber-sécurité, et les difficultés de traçage géographique nécessiterait des mécanismes complexes, issus d'une autorité internationale compétente, ayant le pouvoir de « *maîtriser la frontière électroniqu*e » [92]. En outre, les gouvernements nationaux et leurs réglementations se heurtent régulièrement à la nature même d'Internet : un phénomène mondial, qui échappe aux conflits inter-juridictionnels des états, qui voient leur autorité réduite par la difficulté à appréhender la localisation des acteurs du web. Les créateurs d'Internet, Vint Cerf et Robert Kahn, décrivent les barrières à la régulation en montrant la complexité des canaux de communication. Il n'existe pas de canal centralisant l'ensemble de nos communications électroniques, mais plutôt une multiplicité de réseaux qui transmettent nos messages, eux mêmes subdivisés en « *paquets numériques suivants différents itinéraires de leur sources à leurs destinations* »[93]. Sans une courroie de transmission unique, il est donc extrêmement

[90] Trudel, Pierre « *Quel droit et quel régulation dans le cyber-espace ?* », 2000 Sociologie et Société n°32
[91] Klein, Hans « *ICANN et la Gouvernance d'Internet, la coordination technique comme levier d'une politique publique mondiale* », Les Cahiers du numérique, 2002 p91
[92] Ibid
[93] Cerf, Vinton, Khan, Robert, « *A protocol for packet network interconnection* » IEEE Transactions on Communications v.COM n. 5, Mai 1974 p. 637-648.

complexe d'appliquer une norme unique à cette multiplicité de réseaux. C'est ce que souligne H. Klein, en arguant que la nature « a-spatiale »[94] de l'Internet remet en cause les fondements même de l'autorité publique, qui reposent sur la souveraineté revendiquée par un Etat sur une aire géographique bien délimitée par des frontières physiques. De ces difficultés, on peut noter que trois formes de gouvernements de l'Internet ont progressivement émergé : la production de normes réglementaires par le législateur, l'intervention des pouvoirs publics par la régulation, et la mise en place de dispositifs d'autorégulation en collaboration avec le secteur privé. Ces différents types d'interventions, que nous étudierons plus précisément dans l'analyse du « bien commun de l'Internet », nous mènent à une interrogation en profondeur sur les différences d'approche entre les Etats-Unis et l'Union Européenne sur le rôle des pouvoirs publics dans un tel gouvernement. En novembre 1998, le secrétariat d'état au commerce des Etats-Unis a reconnu officiellement l'ICANN (The Internet Corporation for Assigned Name and Numbers) comme l'organisation ayant la responsabilité de réguler la distribution de noms et de numéros de domaines. Cet acte est capital puisqu'il consacre une approche très particulière de la régulation, le « concept of industry self regulation »[95]. Une association privée à but non lucratif de droit californien se voit ainsi chargée de la gestion et de la coordination des ressources les plus importantes d'Internet, avec une autorité s'étendant à l'ensemble des utilisateurs. Cette idée d'autorégulation a profondément marqué la présidence de Bill Clinton et son approche de l'économie numérique, une « stakeholders approach » basée sur la délégation d'un pouvoir de régulation, normalement dévolue à l'administration fédérale, à une organisation née du consensus entre les différents acteurs du secteur privé. L'ICANN devait ainsi, d'après Milton Mueller, voir l'administration américaine maintenir sa participation à un rôle de soutien technique et administratif pendant deux ans avant de se retirer de l'organisme. Dénonçant d'une part l'instrumentalisation de l'ICANN par le gouvernement américain, et d'autre part l'arrivée d'un acteur puissant le « private sector », il critique vivement le manque de légitimité de cette autorité et conteste son indépendance. [96] L'intérêt d'une telle autorité cependant, c'est son fonctionnement axé sur le contrôle du système de noms de domaine internet ! En effet le DNS étant centralisé, il constitue un possible point de contrôle à partir duquel il est possible à l'ICANN de réguler les utilisateurs, mais aussi de les sanctionner, puisque le refus d'accès aux noms de domaines

[94] Holitsher, Marc « *Debate, Internet Governance* », La revue Suisse de la Science Politique n°5, 1999 p115
[95] Mueller, Milton « *ICANN and Internet governance, sorting through de debris of self regulation* », INFO Vol 1, 6 Décembre 1999
[96] Ibid

équivaut à un bannissement pur et simple d'Internet. Pour expliquer simplement le fonctionnement du DNS, H. Klein utilise une métaphore : celui-ci peut être considéré comme « l'annuaire et les renseignements téléphonique d'Internet »[97]. Lorsque nous utilisons un moteur de recherche en sélectionnant le lien d'une page web ou envoyant un email, le DNS reconnaît le nom de domaine et forme le numéro IP correspondant. Alors que le système de communication, le premier pilier du fonctionnement d'Internet, est très décentralisé puisqu'il s'organise autour de plusieurs protocoles par lesquels des groupes d'ordinateurs indépendants peuvent s'envoyer des données, « l'adressage » (le DNS) est un levier d'action opérationnel pour un organisme de régulation[98]. Ce système, véritable base de données unique, implique la présence d'un administrateur qui « met en œuvre ces décisions, en ajoutant, supprimant, ou modifiant les entrées dans la base de données pour refléter l'entrée, la sortie ou le changement de statut de divers ordinateurs »[99]. Pour que l'ICANN, administrateur du DNS, puisse constituer une véritable puissance régulatrice, il faudrait étendre le champ de ses compétences aux problématiques du copyright ou au contrôle des contenus, ce qui crée un véritable problème de légitimité démocratique de l'organisation. En effet, un grand nombre de pays s'élèvent aujourd'hui contre la « stakeholders approach » qui conditionne l'existence de l'ICANN et sa légitimité, et tant qu'organe représentant les communautés d'utilisateurs identifiées par Pierre Trudel. Dans les années 1990 notamment, la Commission Européenne, l'ITU et les gouvernements nationaux ont commencé à remettre en question le monopole accordé à cette infrastructure informatique mondiale. Cependant, les statuts de l'ICANN sont extrêmement stricts : aucun fonctionnaire ne peut être membre du conseil d'administration, lequel « *exige au minimum une fois par an, une déclaration de la part de chaque administrateur exposant toutes les activités commerciales et autres affiliations ayant trait d'une manière ou d'une autre aux activités commerciales et aux autres affiliations de l'ICANN* »[100], et doit être composé des « *personnes qui formeront la plus large diversité culturelle et géographique au Conseil d'administration, conformément aux autres critères soulignés dans cette section* »[101]. Enfin, l'ICANN précise que les membres de son conseil d'administration doivent être des bénévoles, agissant dans le cadre de l'organisation « *sans*

[97] Klein, Hans « *ICANN et la Gouvernance d'Internet, la coordination technique comme levier d'une politique publique mondiale* », Les Cahiers du numérique, 2002 p91
[98] Ibid Hans Klein
[99] Ibid
[100] Règlements de l'ICANN, Société de droit californien à but non lucratif, Article VI, Section 3 : critères de sélection pour les administrateurs
[101] Ibid

autre compensation que le remboursement certains frais »[102]. Malgré cette séparation claire entre l'organisation et le gouvernement américain, celui-ci conserve un droit de véto sur les décisions politiques de l'ICANN par le biais du Département du Commerce. Etant par ailleurs de droit californien et soumise de ce fait au procureur californien, elle relève en dernière instance de ce même de même département du commerce. Enfin, l'ICANN continue à fonctionner sur la base d'un mémorandum avec ce ministère, incluant la participation du NTIA, qui représente le département américain, au sein du comité de conseil aux gouvernements de l'ICANN. Or, ce mémorandum disposait que cette mise sous tutelle devait prendre fin le 30 septembre 2009, lorsque l'ICANN aurait atteint certains objectifs fixés, par la NTIA[103], et l'organisation n'a toujours pas obtenue son indépendance à l'heure actuelle. En dépit de la privatisation d'internet et de l'autorégulation, les Etats Unis ne souhaitent pas perdre l'emprise qu'ils exercent encore sur l'autorité. On remarque ici une fois encore la différence d'approche entre les législateurs européens, pour qui la protection des données personnelles est un droit fondamental, et l'administration de Bill Clinton, dont la conseillère chargée du e-commerce Ira Magaziner, avait proclamé que « *if the privacy protections by the private sector can be spread internationally, that will become the de facto way privacy is protected* » [104]. L'approche des parties prenantes est donc un moyen efficace de diffuser voir même d'imposer, via un dispositif de sanction et de régulation, la vision américaine de la protection des données.

L'ICANN n'est qu'une des quatre composantes du vaste dispositif imaginé par Vint Cerf et Robert Khan, à la fois pour éviter qu'Internet tombe dans l'escarcelle des Etats, et d'autre part pour garantir la continuité de leur vision d'un Internet à la fois libre d'accès et ouvert. En effet trois organisations interagissent en permanence pour assurer le fonctionnement de disposotif, autour du leitmotiv suivant : « *We envision a future in which people in all parts of the world can use the Internet to improve their quality of life, because*

[102] Ibid

[103] National Telecomunication & Information Departement « *Assessment of the Transition of the Technical Coordination and Management of the Internet's Domain Name and Addressing System* » 24 avril 2009 p1-3

[104] Farrell, Henry, "*Constructing the International Foundations of E Commerce*." International Organization n°57 Printemps 2004 277–306, in « The Global Governance of the Internet (…) » of Daniel Drezner in 2002

standards, technologies, business practices, and government policies sustain an open and universally accessible platform for innovation, creativity, and economic opportunity".", disponible sur la section "Why the Internet matters" du site de la Internet Society. L'ISOC, créee en 1992 a un rôle prééminent dans les discussions et débats concernant la gouvernance du réseau Internet. A ce titre, les membres de l'organisation participent en tant qu'experts à de nombreux sommets internationaux sur le sujet, comme le Forum sur la Gouvernance de l'Internet (IGF) et le Sommet Mondial sur la Société de l'Information (WSIS). Partenaire d'un certain nombre d'organisations internationales et régionales, comme l'OCDE, l'UIT, le Conseil de l'Europe ou encore l'organisation mondiale de la propriété intellectuelle, la Internet Society possède un statut d'observateur et de coordinateur de différents groupes de travail. Reconnue comme une autorité morale et technique, elle travaille avec l'ICANN et l'IETF, la Internet Engineering Task Force (« Détachement d'Ingénierie d'Internet » en français) dont elle est le support instututionnel, qui produit la plupart des standards relatifs à l'internet grâce à une centaine de groupes de travail composés de chercheurs et d'ingénieurs. Enfin, Le W3C (World Wide Web Consortium) constitue l'organisme de normalisation des langages multimédia qui sont utilisées sur sur la toile. Il s'agit d'un club ouvert exclusivement aux organisations qui peuvent acquitter les droits d'adhésion à l'organisme. Cette division de la gouvernance d'Internet dont l'ICANN est le point nodal, révèle une vision américaine profondément marquée par l'autorégulation, même si l'organisation constitue en réalité un cheval de Troie du département de commerce américain pour asseoir l'emprise des Etats-Unis sur le traitement des données et la réglementation des noms de domaines. Pour limiter la captation de l'intérêt général par des intérêts privatifs ou étatistes, il apparaît nécessaire d'imaginer un autre un autre modèle de régulation de l'Internet.

3. Entre autorégulation et réglementation : la solution d'une co-régulation d'Internet ?

Afin de dépasser l'antagonisme entre les partisans de la réglementation, qui estiment qu'elle est le seul processus légitime, émanant d'institutions existantes pour traiter les problématiques juridiques soulevées par le numérique, et les tenants de l'autorégulation, qui estiment que les acteurs privés sont mieux à même d'imposer des codes éthiques et des pratiques de régulations efficaces, la solution d'une gouvernance basée sur la co-régulation a

été avancé par de nombreux auteurs. Eric Brousseau, Professeur à l'Université Paris X Nanterre mets cependant en garde les décideurs contre celle-ci, en utilisant l'exemple de l'ICANN. Pour lui, si co-régulation signifie « *co-intervention sur un pied d'égalité de l'Etat, des entreprises et des groupes d'intérêts dans les procédures de régulation, à l'instar de ce qui se dessine au sein de l'ICANN, alors la co-régulation n'est pas garante d'efficacité, car elle n'organise pas une hiérarchisation des intervenants en fonction de la diversité de la gamme des intérêts* »[105]. Il estime en effet que l'ICANN, sous couvert d'un modèle de communauté et de libre entrée, n'établie pas de domination de l'Etat dans le processus décisionnel. Cependant à l'échelle européenne l'accord institutionnel « Mieux légiférer », publié au journal officiel le 31 décembre 2003[106] défini une liste de critères permettant d'appréhender la co-régulation comme un mécanisme assurant l'adaptation de la législation aux secteurs concernés.

Plus concrètement la délégation de la réalisation d'objectifs précis à des parties expertes dans un secteur donné, comme des opérateurs économiques, des partenaires sociaux ou des acteurs non gouvernementales serait subordonné à l'utilisation du mécanisme de la co-régulation par l'autorité législative. Autrement dit, il n'y a pas dans un tel système d'égalité à proprement parler entre les différentes parties prenantes comme au sein de l'ICANN, mais plutôt une délégation partielle du pouvoir de l'autorité législative à des instances expertes. De plus la Commission constitue le garde fou d'un tel dispositif, le point 17 de l'accord disposant que celle-ci « *veille à ce que le recours aux mécanismes de corégulation et d'autorégulation soit toujours conforme au droit communautaire et qu'il respecte des critères de transparence et de représentativité des parties impliqués* »[107]. Le recours à un tel processus doit également respecter le principe de proportionnalité, et la Commission doit motiver à l'autorité législative compétente les raisons d'un tel recours. Dans le domaine du e-commerce, ces méthodes ont été utilisés à plusieurs reprises en Europe depuis 1995, notamment concernant des accords sur la vente directe et les différends de vente directe, le développement du labels de sécurité du e-commerce, l'organisation de la vente par correspondance et à distance transfrontalière, des

[105] Brousseau, Eric « *Régulation de l'Internet :L'autorégulation nécessite-t-elle un cadre institutionnel* ? » Economie de l'Internet, Revue Economique, Numéro Spécial, Septembre 2001

[106] Parlement Européen, Conseil, et Commission Accord InterInstitutionnel-« Mieux légiférer » (2003/C 321/01), 31 décembre 2003 point 18

[107] Ibid point 17

relevés de bonnes pratiques voire des certifications sur les profils professionnels dans la société de l'information, notamment les prestataires de services sur Internet [108]. Cette utilisation d'un mécanisme européen de la co-régulation, bornée, contrôlée, et soumise à l'approbation de l'autorité législative compétente, est plus protectrice du citoyen que la conception d'une communauté ouverte de l'ICANN, mais laisse moins de place à l'intervention d'experts puisque elle est conditionnée à l'autorisation de l'autorité législative.

[108] Conseil Economique et Social Européen « *L'Etat actuel de la corégulation et de l'autorégulation dans le marché unique* » Les cahiers du CESE, Février 2005 p16

Section II : La donnée : une ressource économique indispensable au marché intérieur

Pour le Professeur Georges Chatillon, l'investissement massif dans le numérique remonte à l'entrée des Etats-Unis dans la seconde guerre mondiale, par le biais de la concentration dans les industries du logiciel de bureau et de PC à la chaîne, et de la favorisation de la concurrence dans le domaines des télécommunications[109]. Selon lui, Internet a été *« le cheval de Troie de la culture politique, économique, financière et commerciale américaine* » par le biais d'un moyen simple : la gratuité. En effet l'avènement de logiciels internet américains dit « libres » a imposé cette vision au reste du monde. Les Etats-Unis en obtenant que les communications électroniques ne soient pas soumises à des taxes ou des droits de douane, ont favorisé le développement à échelle mondiale du commerce électronique. Pourtant malgré, les coups de boutoirs portés au droit d'auteur par cet essor considérable, les Etats-Unis ont tentés de construire leur propre vision du Copyright dans le numérique. Dans une affaire Sony Corporation vs. Universal City Studios Inc, le fabricant de matériel d'enregistrement fut traduit en justice par le fabricant de contenu Universal Studios pour violation du droit d'auteur[110]. Or la Cour Suprême acquitta dans un arrêt d'appel Sony, estimant que non seulement « *la possibilité de dupliquer du matériel vidéo grâce aux nouveaux outils n'entrainerait aucun préjudice pour les ventes de matériel audiovisuel, mais qu'elle procurerait de surcroit aux producteurs un marché secondaire – celui de la vidéo domestique – garantissant des profits identiques si ce n'est supérieurs à ceux des voies traditionnelles*. » [111] Elle considéra donc que les profits apportés par cette nouvelle technologie étaient supérieurs aux pertes occasionnées en terme de droit d'auteur. Plus tard, elle adopta une solution différente, avec des conséquences similaires lors de l'affaire opposant Napster à plusieurs grandes maisons de disques et à la Société américaine des Sociétés

[109]Chatillon, Georges « *L'internet : bien public-bien privé-bien commun* » annuaire de le l'Université Paris I Panthéon Sorbonne

[110] Cour Suprême des Etats-Unis, Sony Corporation vs. Universal City Studios Inc, 464 US 417, 1984

[111]Ramello, Giovanni « *Napster et la musique en ligne, le mythe du vase de Pandore se répéterait-il ?* » Hermès Sciences Publication, 2001, p135

d'Enregistrement. Quand cette application permis en 1999 aux utilisateurs d'écouter librement et immédiatement plusieurs milliers de chansons, satisfaisant d'innombrables insatiables lecteurs par une immense bibliothèques, la Société américaine des sociétés d'enregistrement déposa une plainte très médiatisée, réussissant l'exploit de faire passer le nombre d'utilisateur du site de 200 000 à 57 millions en quelques jours[112]. Le paradoxe, c'est que lorsque le tribunal américain imposa plusieurs limitations d'accès, provoquant la chute progressive de l'utilisation de l'application, les ventes d'albums dégringolèrent aussi. Ce phénomène nous amène à réfléchir sur la question suivante : les droits fondamentaux sont ils un frein pour l'innovation, et si oui, le législateur doit il arbitrer entre impératif d'innovation et protection des citoyens ? L'Union Européenne, sur cette question, a forgé parallèlement à la construction d'un cadre juridique européen de la protection des données, une position très différente de celle des Etats-Unis. Nous aborderons en premier lieu l'impératif d'intervention du législateur pour réguler le marché intérieur du numérique, en décrivant d'abord une approche européenne pluridisciplinaire de la régulation du numérique, puis en montrant les carences de l'agenda numérique. En second lieu, nous étudierons l'arbitrage que doit effectuer la Commission entre la protection des droits fondamentaux et la préservation de la compétitivité des entreprises du numérique. Pour cela, nous montrerons d'abord qu'il y a une véritable spécificité du modèle du e-commerce, où le client est à la fois le consommateur et produit, et dans un second temps nous présenterons les affaires ayant opposé les entreprises Microsoft et Google à la Commission Européenne, profondément révélatrice d'une nouvelle impulsion de la stratégie européenne. Enfin, dans une dernière sous partie, nous démontrerons que la politique de la commission est justifiée par la théorie des infrastructures essentielles.

A. L'impératif d'intervention étatique au sein du marché intérieur du numérique

[112] Lessig, Lawrence « *L'avenir des idées : le sort des biens communs à l'heure des réseaux numérique* » Random House, 2001, p162

1. Une approche européenne pluridisciplinaire de la régulation du numérique

Progressivement, l'Union Européenne a mis en place une approche qui protège le consommateur et le citoyen, mais aussi le marché intérieur. Le règlement sur la protection des données évoqué plus tôt est révélateur d'une réelle volonté du législateur européen de simplifier les formalités administratives de la sécurisation des données pour les entreprises pour créer les conditions d'une amélioration du commerce électronique au sein des Etats-Membres. Une telle politique est la condition sine qua non d'un cadre juridique durable. En effet comme le proclame la Présidente de la CNIL, « *si l'on veut construire une innovation durable, qui ne soit pas rejetée par l'utilisateur, les entreprises doivent apporter des garanties en termes de protection des données personnelles. Ce n'est pas un coût, c'est un investissement »*[113]. Alors que la grande majorité des technologies utilisées aujourd'hui se fonde sur un modèle impliquant la collecte des données dans le but de proposer des publicités ciblées aux consommateurs, on peut aisément qualifier les données de « nouveau capital » de l'économie. En effet plus une entreprise doté d'un tel modèle possédera d'informations sur ses clients, plus elle pourra augmenter ses ventes. Amazon est un très bon exemple d'entreprise faisant de la collecte de la donnée la colonne vertébrale de son modèle de vente, grâce à un algorithme définissant les préférences du consommateur par un système de comparaison[114]. Le consommateur, tout puissant dans ce modèle, troque ses données contre la définition exacte de ses préférences, ce qui permet à l'entreprise de fournir un service qui n'aurais jamais existé autrement. La donnée est donc une ressource économique indispensable au bon fonctionnement du marché intérieur du numérique ! Toutefois il nous appartient de voir à partir part quelle logique le législateur européen à voulu considérer cette donnée. Dans une perspective de libre circulation des données, à laquelle des quatre libertés piliers du marché intérieur peut-on rattacher celle-ci ? En réalité, si il est courant de se rattacher à ces quatre libertés définies à l'article 26 du TFUE[115], qui dispose que « *le marché intérieur comporte un espace sans frontières intérieures dans lequel la libre circulation des*

---

[113] Vincent, Claude, «*La ruée vers l'or des données personnelles*», Enjeux Les Echos, mars 2013

[114] Lessig, Lawrence « *L'avenir des idées : le sort des biens communs à l'heure des réseaux numérique* » Random House, 2001, p165

[115] TFUE, article 26 paragraphe 2, Journal Officiel de l'Union Européenne, 9 mai 2008

marchandises, des personnes, des services et des capitaux est assurée », il ne faut pas négliger l'émergence de régimes spéciaux encadrant la libre circulation des données personnelles, des actes et des décisions de justice, des contrats etc[116]. Le régime spécial applicable à la donnée en Europe, dont nous avons décrit le cadre juridique précédemment, nous empêche de considérer les données à l'aune de la liberté de circulation des capitaux, et oblige la Commission Européenne à favoriser le consensus entre Etats-Membres pour réguler efficacement la ressource économique. Si ceux-ci s'accordent pour encourager la fin des blocages, ils sont beaucoup plus divisés sur l'arbitrage à effectuer entre liberté économique et protection des droits fondamentaux.

2. Un agenda incomplet, révélateur des divisions des Etats Membres

Parmi les objectifs de l'agenda numérique 2020, on ne peut que remarquer le réel consensus politique des Etats Membres autour de mesures fortes comme la bataille contre le géo-blocking, l'encouragement du cloud computing, et la facilitation de la circulation des données. Il est particulièrement intéressant de noter que le droit européen de la concurrence européen est pleinement conforme à l'objectif de créer un marché unique numérique de l'Union Européenne, mais c'est le droit d'auteur qui ouvre la possibilité aux propriétaires d'une œuvre de restreindre géographiquement une licence. A titre d'exemple les studios de cinéma ont le droit d'accorder des licences nationales pour leurs plates formes dans chaque Etat-Membre de l'Union. Plus concrètement : si un contenu a été autorisé sur en Allemagne, il peut être protégé par géo-blocage lorsqu'un utilisateur tente d'y accéder depuis la France. Au stade de l'achat de contenus ou de produits physiques en ligne, le consommateur peut se voir refuser l'accès à un fournisseur de services en ligne dans un autre pays, ou redirigé vers le site web local de la même société avec des prix différents. Le 7 mai 2015, la commissaire à la direction générale de la concurrence, Margaret Vesthager, avait annoncé son attention d'en finir avec ces pratiques de géo-blocage, déclarant « *ne pas comprendre pourquoi elle pouvait regarder mes chaînes danoises préférées sur sa tablette à Copenhague et ne pas en avoir la*

[116] Dubout, Edouard, et Maitrot de la Motte, Alexandre «*L'Unité des libertés de circulation* », Bruylant, Septembre 2013, Avant Propos

possibilité à Bruxelles »[117]. Le communiqué de presse de la commission de la même date sur le marché numérique annonçait d'ailleurs au point 4[118] une intention réelle de stopper « *ces pratiques discriminatoire injustifiée utilisée pour des raisons commerciales »,* qui donnent la possibilité à des plateformes de bloquer l'accès à un site internet à des utilisateurs en raison de leur localisation, ou bien de les rediriger contre leur grès vers un site de vente localisé dans leurs pays affichant des prix différents. Andrus Ansip, vice président pour le marché unique, avait invité à plusieurs reprises en février 2015 l'ensemble des utilisateurs victimes de ce phénomène à lui faire parvenir les captures d'écran des blocages, proclamant que « *dans un vrai marché unique du numérique, chacun doit pouvoir accéder au même contenu licite n'importe où en Europe* »[119]. Il avait par ailleurs rappelé que ce qui est accessible hors ligne devait également l'être lorsque l'utilisateur est connecté à Internet.

Exemple du phénomène du Géo-Blocking sur Youtube :

[120]

Pour illustrer les déclarations de la Commissaire en charge de la concurrence, la commission avait adressé le 23 juillet 2015 une communication de griefs aux principales de

[117] Commission Européenne-Communiqué de Presse, « A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen » 6 mai 2015
[118] Idem point 4
[119]Ansip, Andrus « Thanks for sharing your experience » Twitt du 23 février 2015
[120] Wilson, Matthew « *EU Commission open anti-trust case over geo-blocking* » Kitguru, 24 juillet 2015

studios de cinémas d'Hollywood et à Sky UK, alléguant que les dispositions de géo-blocage introduites dans leurs accords de licence étaient contraires au droit européen de la concurrence. Margaret Vesthager indiquait qu'ils ne « *permettent pas aux consommateurs d'autres pays de l'UE d'accéder aux services de télévision payante britanniques ou irlandais de Sky, que ce soit par satellite ou en ligne* »[121]. Cette volonté politique de la Commission fait suite à une jurisprudence constante de la Cour sur le géo-blocage. En 2011, dans l'arrêt Footbal Association Premier League Ltd et Karen Murphy la CJUE s'étaient penchée sur le phénomène des restrictions territoriales absolues figurant dan les accords de licence relatifs à des services de télédiffusions[122]. En l'espèce, les radios diffuseurs s'engageaient dans le contrat de licence conclu avec la FAPL, à crypter son signal satellite et à le transmettre aux seuls abonnés du territoire qui lui avais été attribué. Suite à plusieurs tentatives de contournement de cette exclusivité par des dispositifs de décodages étrangers, la High Court avait saisi la CJUE sur plusieurs questions d'interprétation du droit de l'Union. La cour avait alors considéré qu'une disposition interdisant à un diffuseur par satellite de diffuser ses programmes à des consommateurs se trouvant en dehors de la zone couverte par la licence était contraire à l'article 56 du TFUE. De plus, elle permettait à tout diffuseur d'obtenir l'exclusivité absolue d'un territoire, éliminant ainsi toute concurrence. Le juge et le législateur s'accordent donc sur la nécessité de mettre un coup d'arrêt au phénomène du géo-blocking qui pénalise le consommateur. Cependant, ces verrous technologiques sont également une des clés de financement de l'industrie culturelle, et une barrière contre les géants américains du numérique, provoquant un réel débat. Constance le Gripp, député PPE, avait manifesté son agacement à la lecture du rapport de l'Eurodéputée du parti pirate Julia Reda sur l'adaptation de la directive des droits d'auteurs, en pointant le danger de la fin des barrières géographiques. Selon elle, « *cela va favoriser les grands acteurs étrangers, car être obligé d'acheter des licences paneuropéennes serait pour beaucoup insurmontable* »[123].Concernant les contrats de licence, on constate une fois encore la difficulté des législateurs à réaliser une

---

121 Commission Européenne-Communiqué de Presse « Pratiques anticoncurrentielles: la Commission adresse une communication des griefs concernant la prestation transfrontière de services de télévision payante disponibles au Royaume-Uni et en Irlande », 23 juillet 2015

122 CJUE arrêt Football Association Premier League Ltd et Karen Murphy, affaires jointes C-403-8 et C-429-8, 4 octobre 2011

123 Rees, Marc, « *Droit d'auteur, l'Europe veut s'attaquer au geoblocking* », Next Impact, 23 février 2015

véritable harmonisation, préférant un protectionnisme larvé et une législation morcelée à la concurrence des géants américains du numérique.

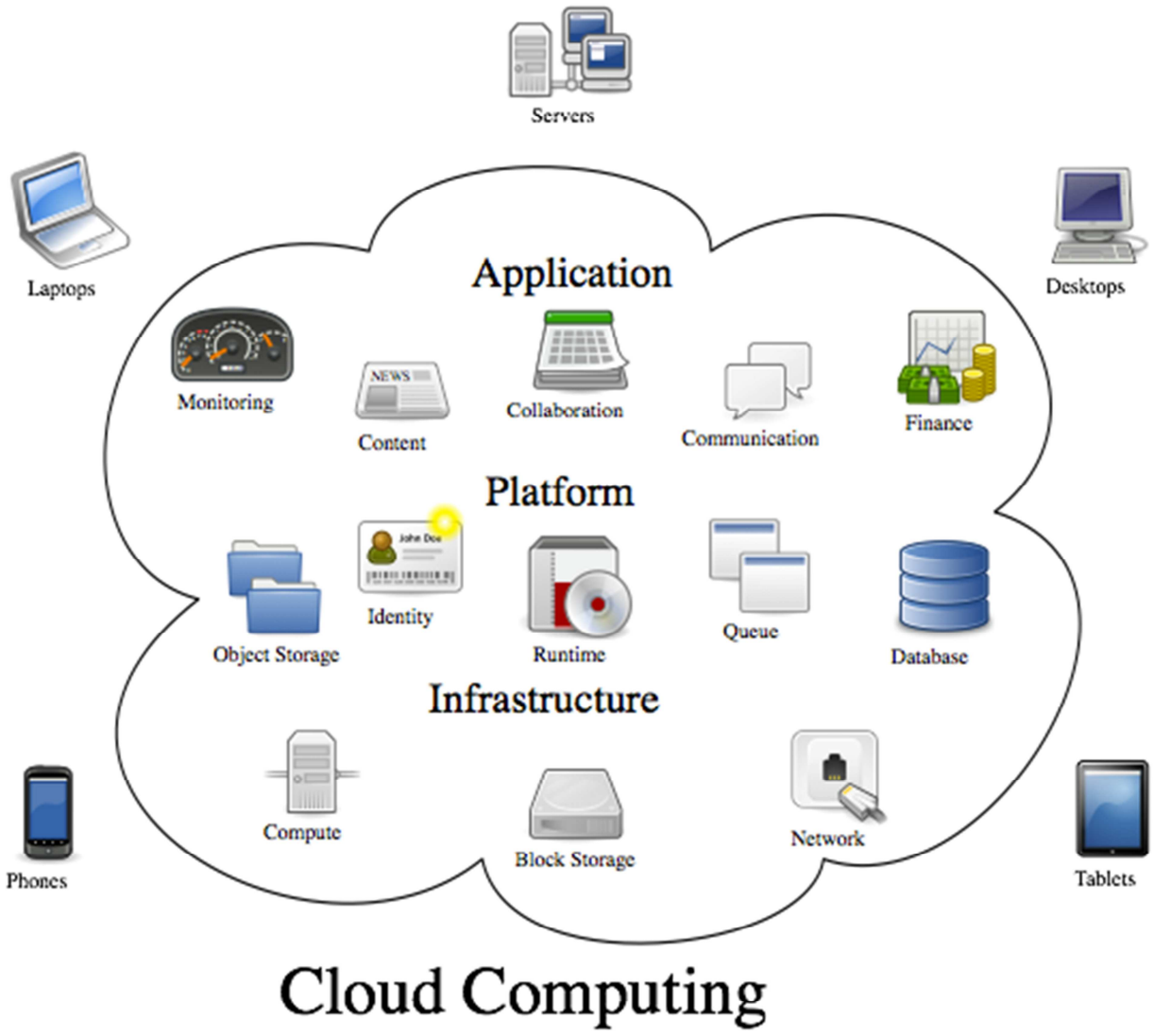
Parmi les priorités de la Commission qui concernent les données des citoyens européens, le Cloud computing occupe également une place prépondérante. Le Cloud Computing ou nuage informatique, est un moyen moderne de partager et de stocker des informations par internet, permettant d'accéder directement à ses données avec un simple portail web. Il s'articule autour de quatre critères clés : la mutualisation des ressources, le modularité, le paiement à l'usage, et la conformité. Comme on peut le voir ci-dessous, c'est un formidable outil de stockage pour lequel la commission européenne avait exprimé son intérêt par une communication du 27 septembre 2012 au Parlement Européen, au Conseil, au Comité Economique et Social Européen, et aux comités de région titrant « Unleashing the Potential of Cloud Computing in Europe »[124]. Cette communication représentait un premier engagement de la Commission Européenne signifiant une augmentation considérable des dépenses liées au nuage informatique, accompagné d'un impact sur l'économie de 975 milliards d'euros, et d'un gain de 3,8 millions d'emploi en 2020[125]. Une enquête de la commission européenne de 2011 montrait qu'adopter le nuage européen permettrait à 80% des entreprises de réduire de 10 à 20% de leurs coûts[126]. En dehors de la commission européenne, nombreuses sont les études faisant l'éloge de l'efficacité de ce dispositif de stockage. A titre d'exemple un rapport du CIGREF, une association d'entreprises françaises spécialisée dans la maitrise des enjeux numérique par les entreprises pointait deux choses[127]. Premièrement, le fait que l'informatique en nuage pouvait être l'occasion pour les pouvoirs publics de favoriser l'émergence de start-ups et de champions nationaux par le biai d'initiatives ciblées comme des plans d'investissement en compétences et en infrastructures. Deuxièmement, l'idée que l'Etat Français et les autorités européennes devaient légiférer autour de ce nouvel instrument, afin de veiller sur la sécurité numérique des entreprises. Cette étude pointait notamment la nécessité de rassurer les entreprises de secteurs sensibles sur la localisation de l'information et des données par la création de labels et de certifications, et la

[124] Commission Européenne-Communication « Unleashing the potential of Cloud Computing in Europe » 27 septembre 2012
[125] Ibid
[126] Elyan, Jean « *Cloud computing : la commission européenne appelle à plus de normalisation* » Le Monde Informatique, 25 septembre 2012
[127][127] CIGREF « La réalité du Cloud dans les grandes entreprises » 9 octobre 2015

mise en place d'une réglementation stricte sur les données personnelles[128]. En effet, il est intéressant de 65% des représentants de ces entreprises s'estimaient préoccupés par la sécurité et la confidentialité des donnés envoyées dans le nuage en informatique. Or ces doutes génèrent un questionnement réel sur l'étendue du périmètre du risque « donnée » et la capacité des entreprises à faire confiance aux éditeur de logiciels de Cloud Computing[129]. La sous exploitation de cette technologie est véritablement due à un manque apparent de sécurisation de la donnée par le législateur. En 2015, la mise en avant de cette problématique au Consumer Electronic Show de Las Vegas a montré que les éditeurs de logiciels n'avaient pas encore intégrés dans leurs offres les revendications des entreprises concernant la protection de leur patrimoine numérique, générant une défiance à l'égard de celles-ci.

Fonctionnement du Cloud-Computing :

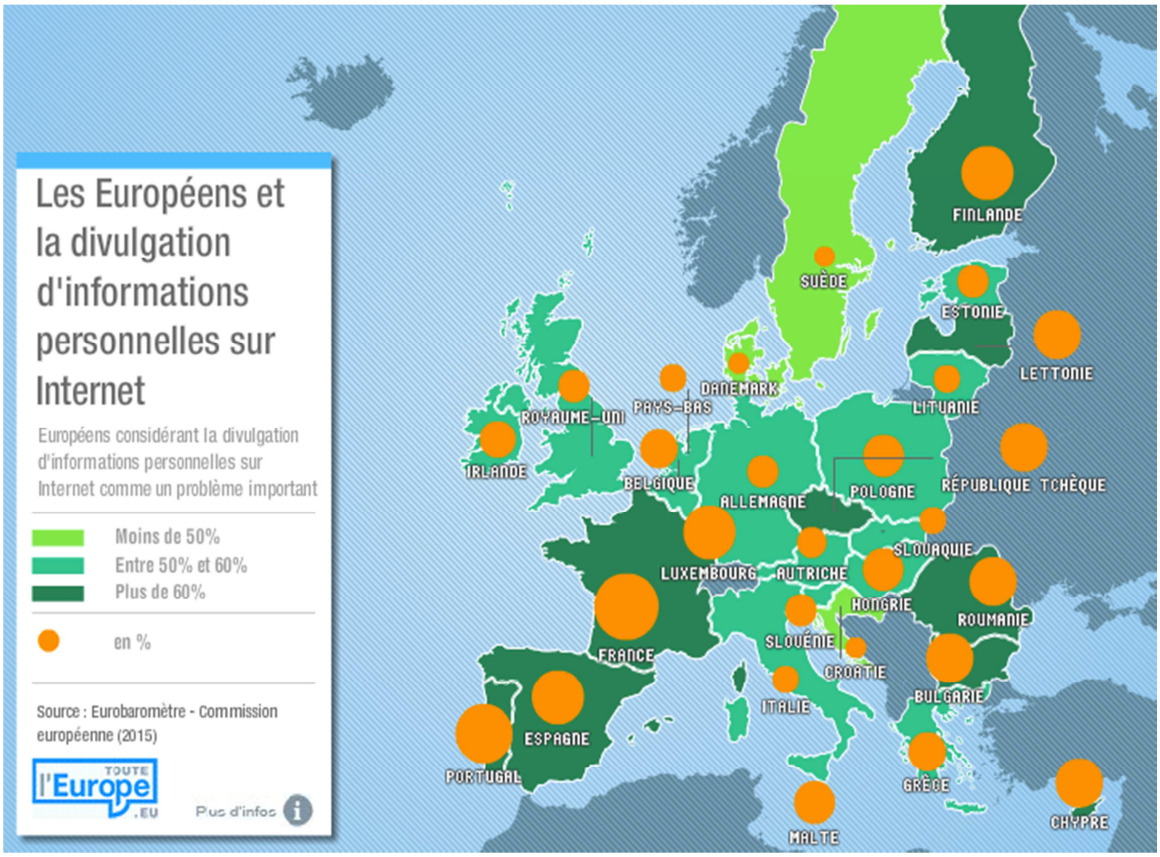
130



B. La conciliation entre libertés fondamentales et compétitivité des acteurs

D'après plusieurs sondages disponibles sur l'eurobaromètre 431, les citoyens européens apparaissent de plus en plus concernés par l'utilisation de leurs données par des entreprises privées. En effet comme on peut le constater sur la carte ci-dessous, ils sont en France, en Espagne, en Roumanie et en Finlande plus de 60% à considérer la divulgation d'informations personnelles sur Internet comme un problème important.

Carte Eurobaromètre 431 « Les Européens et la divulgation d'informations personnelles sur Internet » :



131

Lors de l'obtention de l'accord entre le Comité LIBE du Parlement Européen, le Coreper et la Commission Européenne sur la réforme européenne de la protection des données personnelles le 22 décembre 2015, Isabelle Falque-Pierrotin, Présidente du G29 et de la CNIL, avait déclaré : « *Par cet accord, l'Europe marque sa détermination à être un acteur majeur du numérique tout en préservant les valeurs humanistes qui sont les nôtres. C'est un signal envoyé à tous les acteurs mondiaux. Le niveau de protection des données des citoyens et consommateurs européens devra rester au moins équivalent à celui garanti par le règlement pour toute entreprise dont les utilisateurs sont situés dans l'Union Européenne*»[132]. Cet accord, première étape de l'aboutissement du règlement européen de la protection des données, fait suite à une réelle prise en compte des inquiétudes des citoyens par les législateurs. Le 19 janvier 2016, le Parlement Européen avait adopté la résolution 2015/2147(INI) « Vers un acte sur le marché numérique », appelant la Commission à évaluer la nécessité de protéger consommateurs de l'économie collaborative. Les députés ont insistés dans cette résolution sur le moteur de croissance que constituait l'économie numérique dans le point 101 de sa résolution : « *estime que l'économie fondée sur les données constitue un élément clé de la croissance économique; souligne que les nouvelles technologies de l'information et des communications (TIC), telles que les méga données, l'informatique en nuage, l'internet des objets, l'impression en 3D et d'autres technologies peuvent offrir des possibilités à l'économie et à la société, notamment si elles sont intégrées à d'autres secteurs (…)* [133]». Ils ont également appelé à une réelle harmonisation autour de la régulation du commerce en ligne, estimant au point 15 qu'une « *harmonisation plus grande du cadre juridique régissant la vente en ligne entre un professionnel et un consommateur de contenu numérique et de biens matériels (…) constitue une approche pratique et proportionnée; insiste sur le fait que cela devrait être fait d'une manière technologiquement neutre et ne pas imposer de coûts déraisonnables pour les entreprises »* [134]. Les membres du Parlement pointent ici une problématique réelle: les 28 Etats Membres ont tous à ce jour des approches

[131] Rapport Eurobaromètre 431, 8 juillet 2015
[132] Falque-Pierrotin, Isabelle « Consensus sur le Paquet Européen Protection des données personnelles » Communication de la CNIL, 22 décembre 2015
[133] Parlement Européen, Résolution 2015/2147 « Vers un acte sur le marché numérique » 19 janvier 2016, point 101
[134] Ibid point 15

de régulation extrêmement différentes ce qui freine le développement de nouveaux business émergents pour la vente de biens et services en lignes. En complément d'un agenda numérique à la fois « pro-marché » et restreint, le Parlement à exprimé par cette résolution une volonté de protéger le citoyen européen, qui tend à oublier que la gratuité de l'utilisation d'Internet est conditionné au fait qu'il est doublement essentiel aux entreprises du e-commerce, puisqu'il est à la fois le consommateur et le produit. L'économie collaborative n'ayant pas été retenue comme une des priorités de la Commission dans son agenda numérique, cette résolution révèlent une fois encore les différences de vues entre l'institution et le Parlement.

1. Le modèle du e-commerce, un client a la fois consommateur et produit

Chaque jour, le coût du commerce électronique tend à se rapprocher de zéro. Chris Anderson, rédacteur en chef de la revue spécialisée Wired, estime que *« tout ce que le numérique touche évolue vers la gratuité (…) D'une certaine manière, le web étend le modèle économique des médias à toutes sortes d'autres secteurs économiques* »[135]. Développant l'idée selon laquelle la gratuité est l'avenir de l'économie, il illustre ce propos en pointant la gratuité de la plupart des albums musicaux, jeux et logiciels de Google comme Google Maps, Gmail et Youtube disponibles en libre accès sur Internet. Il apparaît en effet que dans plusieurs domaines, le passage à la gratuité a participé à la hausse considérable du profit de certaines entreprises. A titre d'exemple, l'évolution du coût du web mail, illustré par le graphique de la page 61, a montré l'efficacité de la politique de Yahoo, qui offre aux consommateurs depuis 2007 une capacité de stockage à la fois gratuite et illimité sur leurs serveurs mails. Cette inflation de la gratuité nous amène à une interrogation réelle sur la contrepartie obtenue par les entreprises en échange de cette offre aux consommateurs. La réponse est simple : le donnée est la matière première d'un modèle de e-commerce où l'entreprise se rémunère par la collecte des informations du consommateur, puis leurs ventes. D'après une étude réalisée par le Boston Consulting Group, il est aujourd'hui possible d'estimer la vie personnelle d'un citoyen de l'Union Européenne a 600 euros, une valeur qui

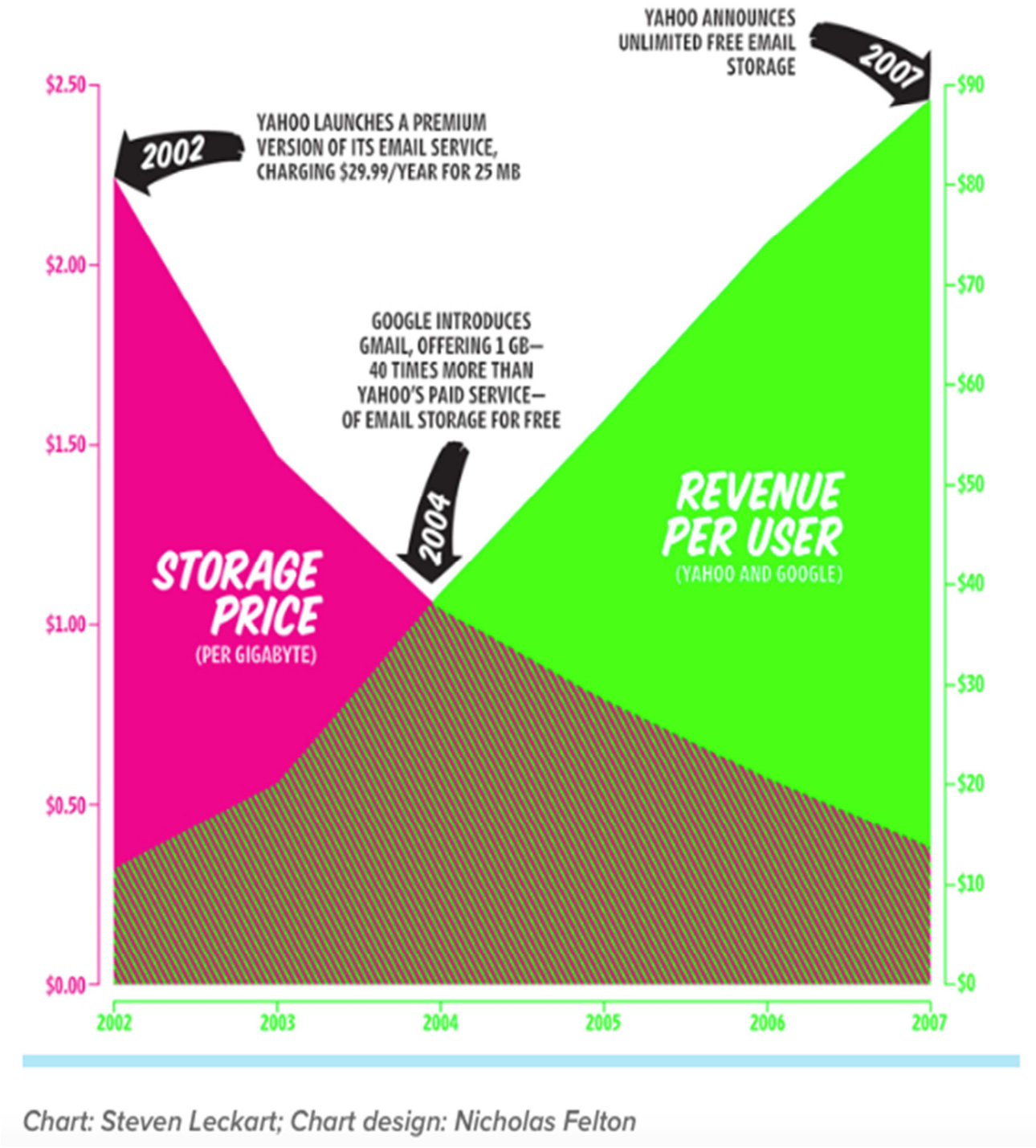
[135] Anderson, Chris dans l'article de Guillaume, Hubert « *La gratuité est-elle l'avenir de l'économie ?* » Internet Actu, 10 mars 2008

serait amener à tripler en 2020[136], une valeur significative du peu d'intérêt qu'aurait une entreprise à restreindre l'utilisation de son application à un abonnement, alors qu'un consommateur lui rapporte bien plus par ses informations personnelles. Dans un tel modèle, c'est la loyauté des plateformes envers le consommateur qui compte. En effet les règles de confidentialité internes sont la seule protection contre la dérive de la régie publicitaire de Facebook et Google, ou la vente intensive de biens et de services d'Apple et d'Amazon[137].

[136] Boston Consulting Group « The Value of our digital identity » November 2012, p17-18
[137] Vincent, Claude « La ruée vers l'or des données personnelles » Les Echos, 7 mars 2013

Evolution du coût du webmail :

138



138 Chris Anderson « Webmail Windfal » Wired 25 février 2008

Ce modèle de e-commerce, centré sur la captation de la confiance et de l'intérêt du consommateur, implique donc que la gratuité à un prix. Or l'Union Européenne, par l'abaissement des barrières du numérique, sert les intérêts de ces acteurs. En effet dans un discours du 26 mars 2015, Margrethe Vestager avait vivement dénoncé le paradoxe du marché intérieur européen qui permet aux consommateurs d'acquérir des biens d'un Etat Membre à un autre, mais laisse subsister des blocages numériques restreignant les possibilités d'acquérir ces mêmes biens en ligne[139]. Elle avait également insisté sur le potentiel du marché unique du numérique, dont le bon fonctionnement pourrait ajouter 340 milliards d'euros au PIB annuel de l'Union Européenne, moyennant l'abaissement des barrières étatiques et la fin de l'utilisation du geo-blocking. Toutefois, cette harmonisation des 28 législations autour du marché unique du numérique ouvre un boulevard aux grands acteurs américains des secteurs qui ont vocation, par un modèle économique centré sur la gratuité du service à s'étendre.

2. Les affaires Google et Microsoft : des arrêts révélateurs d'une nouvelle impulsion européenne

Dans le contexte d'opposition frontale de la nouvelle Commission Européenne sur la question de la souveraineté du numérique, il est judicieux d'étudier la stratégie européenne à l'aune du droit de la concurrence. La politique de concurrence est en effet l'une des prérogatives de l'Union depuis son commencement, ce qui en fait un instrument stratégique de la commission. Cette délégation des états membres a été consacrée par une réglementation de 1962 qui a centralisé les pouvoirs antitrust au sein de la Commission européenne, lui accordant le droit d'enquêter sur les ententes qui pourraient entraver le commerce entre les États-membres et empêcher la concurrence dans le marché commun. Celle-ci dispose pour cela de différents outils et instruments juridiques. L'article 101 du TFUE interdit les décisions d'associations d'entreprises et les accords entre entreprises anticoncurrentiels et l'article 102 du même traité interdit les abus de position dominante susceptibles d'affecter le commerce et d'empêcher ou de restreindre la concurrence[140]. La mise en œuvre de ces dispositions est

[139] Commission Européenne-Discours de Margrethe Vesthager « Competition policy for the Digital Single Market: Focus on e-commerce » 26 mars 2015

[140] Traité sur le Fonctionnement de l'Union Européenne, articles 101 et 102

définie dans le règlement sur les ententes et abus de position dominante[141], qui peut être appliqué par la Commission et par les autorités nationales de concurrence des États membres de l'UE. L'article 11, paragraphe 6, de ce règlement prévoit qu'une fois que la Commission a ouvert une procédure, les autorités nationales de concurrence ne peuvent plus appliquer les règles de l'UE en matière de concurrence aux pratiques concernées. En outre, l'article 16, paragraphe 1, du même règlement prévoit que les juridictions nationales ne peuvent prendre aucune décision qui irait à l'encontre d'une décision prévue par la Commission dans le cadre de procédures formellement ouvertes. Ces dispositions des traités et ce règlement donnent à la Commission un véritable pouvoir d'intervention sur les marchés européens, que Margrethe Vesthager met aujourd'hui au service des objectifs de la nouvelle équipe Juncker. Avant d'analyser l'affaire opposant actuellement Google à la Commission Européenne, il convient d'évoquer l'affaire ayant opposé Microsoft à cette dernière en 2007, révélatrice de la stratégie économique de la Commission.

Dans cette affaire, la Commission agissait en tant qu'autorité de concurrence et avait estimé que l'entreprise avait enfreint les règles du droit communautaire, et avait notamment exigé de Microsoft qu'elle ouvre à ses concurrents d'un certain nombre de données relatives à son système d'exécution. Plus précisément, la commission estimait alors que l'entreprise avait violé l'article 82 CE (actuellement article 102 du TFUE) en commettant des abus de position dominante du fait de deux comportement distincts. D'abord en refusant de fournir à ses concurrents certaines informations relatives à l'interopérabilité et d'en autoriser l'usage pour le développement et la distribution de produits concurrents aux siens sur le marché des systèmes d'exploitation pour serveurs de groupe de travail. Ensuite la vente liée du système d'exploitation Windows pour PC et du le lecteur Windows Media Player,qui a eu pour conséquence une distorsion de la concurrence. [142] En l'espèce la société Sun Microsystems concurrent de Microsoft avait déposé une plainte en 1998 auprès de la DG concurrence de Bruxelles. En effet, Microsoft avait exprimé son refus d'accorder à son concurrent la possibilité d'obtenir des informations techniques sur son système d'exploitation de manière à rendre les systèmes d'exploitation des serveurs pour groupe de travail interopérables avec les PC. L'argument principal de l'entreprise Sun Microsystems, c'est que dans la mesure où le système d'exploitation Windows équipe 90 % des ordinateurs individuels dans le monde,

[141] Règlement n°1/2003 du Conseil de l'Union Européenne, article 11, paragraphe 6
[142] Commission Européenne, Service juridique T-201/04 Microsoft-abus de position dominante : « Concurrence-Microsoft-Abus de Position dominante » 17 septembre 2007

l'entreprise doit avoir accès à un certain nombre de données techniques relatives à Windows pour développer ses propres systèmes d'exploitation pour serveurs pour groupes de travail. Il convient de préciser que ces systèmes permettant aux ordinateurs individuels de fonctionner "en réseau" fonctionnant parfaitement avec des ordinateurs individuels équipés de Windows. A la suite de cette plainte, la Commission Européenne a ouvert une procédure d'infraction aux règles de la concurrence sur la base des griefs démontrés par l'entreprise plaignante. Elle a retenu deux griefs, fondés sur la violation de l'article 82 du Traité CE, après avoir rappelé que Microsoft occupait une position dominante sur le marché des systèmes d'exploitation des PC avec 90% de part de marché, et également sur le marché des systèmes d'exploitation pour serveurs pour groupe de travail avec 60% de part du marché. Elle avait premièrement souligné que le refus de Microsoft à ses concurrents de satisfaire des demandes d'information techniques sur le système d'exploitation Windows, empêchant la concurrence d'assurer l'interopérabilité constituait un abus. Elle avait également noté que le fait d'avoir subordonné la fourniture du système d'exploitation pour PC Windows à l'acquisition simultanée du logiciel lecteur multimédia Windows Media Player restreignait la concurrence sur le marché des multimédias. On parle ici d'un grief dit de « vente lié », à savoir la liaison de la vente de deux produits distincts d'une même entreprise qui limite considérablement la liberté de choix du consommateur. On peut noter ici que cette affaire Microsoft a une importance significative pour le droit de la concurrence puisqu'elle a permis de dégager des critères d'identification du phénomène de vente lié. En premier lieu, la Commission a dégagé deux critères matériels : le produit liant et le produit lié doivent être deux produits distincts et les consommateurs ne doivent pas pouvoir acquérir le produit liant sans le produit lié. Pour qu'une sanction soit prononcée par la suite, trois critères supplémentaires doivent être remplis : l'entreprise concernée doit détenir une position dominante en principe sur le marché du produit liant , la pratique en cause doit restreindre la concurrence, et enfin la vente liée en cause ne doit pas être objectivement justifiée, en particulier par des défenses d'efficience.[143]A la suite du constat de ces abus, la commission a alors infligé la plus lourde amende jamais prononcée à l'encontre d'une seule entreprise, à savoir une somme de plus 497 millions d'euros, [144] assortie de l'injonction de cesser ses pratiques de ventes liées et de mettre à la disposition de la concurrence les informations techniques nécessaires pour assurer

[143] Vogel, Joseph « *Comment apprécier les ventes liées en matière de droit la concurrence* », 14 avril 2010, Droit et Economie, Concurrences n°3-2°2010

[144] Décision de la Commission, relative à une procédure d'application de l'article 82 du Traité CE, du 24 mars 2004 (affaire COMP/C-3/37.792 Microsoft), JOUE, 6 février 2007, L 32/23.

l'interopérabilité de Windows avec les systèmes d'exploitation pour serveur pour groupe de travail. Elle a aussi décidé de nommer un mandataire indépendant dont le nom serait proposé par Microsoft et les coûts afférents à la mission de celui-ci supportés par l'entreprise. A la suite de cette condamnation, Microsoft a formé un recours auprès du TPICE qui a rendu son verdict 3 ans plus tard. Sur la question du mandataire d'abord, le Tribunal a donné raison à Microsoft qui critiquait le fait que la Commission décharge sur un tiers ses obligations d'autorité de la concurrence. Le juge a également pris soin de rappeler que « *le fait pour une entreprise détenant une position dominante, de refuser d'octroyer une licence pour l'utilisation d'un produit couvert par un droit de propriété intellectuelle ne saurait constituer en lui-même un abus de position dominante*"[145]. Il a également rappelé que, partant, « *il est permis dans l'intérêt public du maintien d'une concurrence effective sur le marché, d'empiéter sur le droit exclusif du titulaire du droit de propriété intellectuelle en l'obligeant à consentir des licences aux tiers qui cherchent à entrer sur ce marché ou à s'y maintenir*"[146], et surtout que le refus d'une entreprise de donner des informations techniques constituent un abus seulement en cas de circonstances exceptionnelles. Ces dernières sont caractérisées quand les conditions cumulatives suivantes sont réunies, autour de trois refus : celui de fournir les informations ou de concéder la licence portant sur un produit ou un service indispensable pour l'exercice d'une activité donnée sur un marché voisin de celui sur lequel l'entreprise est en position dominante, celui qui est de nature à exclure toute possibilité de concurrence sur ce marché voisin, et celui qui fait obstacle à l'apparition d'un produit nouveau pour lequel il existe une demande potentielle du consommateur. [147] Le juge ayant identifié ces circonstances, il a rejeté le recours de Microsoft.

Cet arrêt apparaît comme fondateur pour plusieurs raisons. Si la Commission Européenne peut s'autosaisir en tant qu'autorité de la concurrence, elle n'en demeure pas moins le pouvoir exécutif de l'Union Européenne. On peut considérer cette affaire comme une victoire politique dans la guerre commerciale face aux Etats-Unis, d'autant plus que Microsoft et Sun Microsystems sont toutes deux des entités de droit américain, et que cette dernière a pourtant choisi de porter le grief devant la Commission Européenne. D'autre part, certains commentateurs s'interrogent sur un autre aspect de l'arrêt, l'ouverture d'un précédent

[145] TPICE, Affaire T-201/04, Microsoft Corp. contre Commission des Communautés européennes, 17 septembre 2007, Point 331 de l'arrêt
[146] Point 691 de l'arrêt
[147] Vannini, Claire « *L'Affaire Microsoft : le droit de la concurrence saisi par le politique* », Fondation Robert Schuman, 19 novembre 2007

montrant une utilisation « politique » du droit de la concurrence. Pour autant, est-ce que cette nouvelle utilisation du droit ne privilégie pas le dogme du respect de la concurrence par rapport à l'impératif d'innovation ? Selon Eric Caprioli et Anne Cantéro, « *ce n'est alors plus l'interopérabilité qui est au coeur du débat mais l'appréciation d'un abus de position dominante qui se traduirait par une stratégie de développement fondée sur une innovation protégée* »[148]. Par conséquent, en raison d'une approche du droit de la concurrence qu'on pourrait qualifier de politique, la décision rendue par le Tribunal de Luxembourg implique un frein à l'innovation. D'autre part à la suite de la décision de la Commission Européenne, Microsoft a proposé une version de son système d'exploitation sans le logiciel multimédia sur le marché, choisie par 1% des consommateurs seulement d'après les chiffres de Microsoft. Cette proportion affaiblit considérablement l'argument selon lequel les velléités anti-concurrentielles de la Commission européenne seraient justifiées par l'intérêt du consommateur. Comment alors concilier protection du consommateur et innovation du secteur, si l'intérêt du premier dépend de la recherche de modernisation perpétuel du second ? Selon Eric Caprioli la décision du TPICE pouvait avoir deux incidences. D'une part, « *de nouvelles actions contre les entreprises en situation de position dominante* », considérablement facilitées par l'assouplissement des critères de qualification de l'abus. D'autre part, une véritable remise en question des stratégies de recherches et développement des entreprises leaders du numérique[149]. La prémonition de cet avocat s'est révélée exacte puisque 2 ans plus tard, la société Intel Corporation a été condamnée à verser une amende de 1,6 milliards d'euros pour infractions aux règles antitrust du traité relatives à l'abus de position dominante[150]. La sanction confirmée lr jeudi 12 juin 2009 par le Tribunal de l'Union, qui a rejeté l'appel d'Intel en arguant qu'aucun des arguments avancés par l'entreprise ne permettait de conclure au caractère disproportionné de la décision et que « *au contraire, il y a lieu de considérer que cette amende est appropriée aux circonstances* »[151]. Cette décision de la cour, profondément politique, est révélatrice comme dans l'affaire Microsoft de la mise en place par le biais du droit de la concurrence d'un protectionnisme européen tendant à freiner la fois la domination des entreprises américaines. L'affaire opposant Google à la Commission, qui devrait rendre son enquête dans les prochaines semaines, est également

[148] Caprioli, Eric « *L'Affaire Microsoft : concurrence versus innovation* ? » Journal du Net, 9 octobre 2007
[149] Ibid
[150] Article 82 CE
[151] TPICE, Arrêt dans l'affaire T-286/09 Intel Corp/ Commission, Communiqué de Presse n°82/14 p312 juin 2014

significative, et nous amène à nous pencher sur la construction progressive d'un régime de répression des abus de position dominante.

A la suite d'une enquête ouverte en novembre 2010, la Commission Européenne a adressé une communication de grief en avril 2015 à l'entreprise Google pour abus de position dominante[152]. Cette dernière est accusée par la Commission Européenne soutenue par une trentaine d'entreprises plaignantes de favoriser dans les résultats de son moteur de recherche les résultats de ses propres services commerciaux et publicitaires. Il convient de préciser ici la notion d'abus de position dominante, définie le 13 février 1979 dans l'affaire Hoffman Laroche de la manière suivante comme : « *une notion objective qui vise les comportements d'une entreprise en position dominante qui sont de nature à influencer la structure d'un marché ou, à la suite précisément de la présence de l'entreprise en question, le degré de concurrence est déjà affaibli et qui ont pour effet de faire obstacle, par le recours à des moyens différents de ceux qui gouvernent une compétition normale des produits ou services sur la base des prestations des opérateurs économiques, au maintien du degré de concurrence existant encore sur le marché ou au développement de cette concurrence »*[153]. Dans la présente communication, on trouve parmi les entreprises plaignantes plusieurs fournisseurs d'accès à Internet européens, et l'entreprise Microsoft. Parmi les motifs de cette communication de grief, la commission a choisi de se concentrer sur deux aspects. Le premier c'est la mise en évidence systématique par Google de son propre produit de comparaison de prix, « Google Shopping », ce qui entraîne des conséquences sur le marché des produits de comparaison puisque Google n'applique pas le système de pénalités qu'il applique aux autres services du même type. Il est important de souligner ici la dimension profondément politique d'une telle décision. Une fois encore, la Commission Européenne considère d'abord les moteurs de recherche et Google en particulier comme des plateformes supportant l'économie entière. En ce sens, elle a une vision relevant de la tradition française, tendant à considérer Google comme un service public. Le deuxième aspect de la communication de griefs, ce sont les doutes constitués autour des accords entre Google et le système d'exploitation Android.

---

[152] Communication de la Commission, « Abus de position dominante: la Commission adresse une communication des griefs à Google au sujet du service de comparaison de prix et ouvre une procédure formelle d'examen distincte concernant Android » 15 avril 2015

[153] CJUE, 13 février 1979 Arrêt Hoffman-La Roche & Co.Ag contre Commission des Communautés Européennes 85/76, point 6

Ces doutes ont menés à une procédure formelle d'examen distincte de la communication de grief. Depuis 2005 Google a soutenu le développement du système d'exploitation pour appareil mobile Android qui est devenu ces dernières années le premier système d'exploitation de l'EEE, distançant Windows Phone et l'IOS d'Apple et raflant environ 75% du marché des tablettes et des téléphones. Or ce système fonctionne souvent avec un éventail d'applications et de services dont Google est propriétaire, comme Youtube ou Gmail, depuis les accords passés entre le moteur de recherche et le système d'exploitation. L'enquête de la commission, qui se poursuit à l'heure actuelle, est centrée sur les questions suivantes : En premier lieu, l'entreprise Google a-t-elle obligé ou incité les fabricants de téléphones et tablettes à préinstaller exclusivement ses applications et ses services ? En second lieu, Google a-t-elle empêché ces mêmes fabriquant de commercialiser des versions potentiellement concurrentes d'Android? Enfin Google a-t-elle illégalement entravé le développement et l'accès au marché des applications et services de ses concurrents en liant ou groupant certains de ses services et applications distribués sur des appareils Android avec d'autres applications ? Si l'enquête se termine, Google pourrait se voir infliger une amende s'élevant à 10% de son chiffre d'affaire annuel de 74,5 milliards d'euros, reléguant à la portion congrue la sanction encourue par Microsoft en 2007.

Cette communication nous amène à une véritable interrogation quand à la stratégie économique qui sous-tend l'orientation des décisions stratégiques de la Direction générale de la concurrence au sein de la Commission européenne. À ce sujet, l'institut économique Molinari a récemment alerté l'opinion publique sur *« les dangers de l'activisme de la Commission dans la concurrence numérique* ». L'Insitut fait en effet le constat d'une hausse considérable du montant des amendes de la DG Concurrence depuis le début du siècle, atteignant 1,69 milliard d'euros en 2014 au lieu des 3 millions d'euros exigés en 1964[154]. À elle seule, la pénalité d'Intel en 2009 était de 1,06 milliard d'Euros, ce qui nous amène nous interroger sur les velléités politiques de la Commission Européenne envers les acteurs du secteur (Institut Economique Molinari, 2015**).** L'institut propose un plaidoyer en faveur d'un changement de la politique européenne en matière de concurrence en se fondant sur les observations suivantes : «*Les études portant sur l'intégration verticale du type de celle pratiquée par Google à partir de son moteur de recherche horizontal et de ses moteurs de recherche verticaux spécialisés montrent qu'en général une telle intégration est bénéfique*

[154] Institut Economique Molinari « *Google versus Microsoft : du pareil au même ?* » 3 mai 2016

pour les consommateurs. De manière similaire, le biais autoréférentiel dont Google est accusé dans le cas spécifique de Google Shopping peut avoir un impact positif ou négatif sur le bien-être du consommateur. » L'Institut souligne par ailleurs que les parts de marché de Google ont décliné au cours des cinq dernières années, ce qui a favorisé la concurrence et l'arrivée de nouveaux acteurs dans le marché spécialisé de la recherch*e.* Cette étude montre le caractère discutable des arguments économiques avancés par la Direction générale de la concurrence et remet en cause sa méthodologie pour l'établissement d'un état de concurrence dans les marchés concernés. La DG concurrence aurait en effet une tendance marquée à souhaiter juguler « *les forces du marché* », ce qui est contestable au vu des effets de ses restrictions sur les consommateurs. Dans le cas de Microsoft, le temps que le dégroupage imposé par la commission entre en application, une version de Windows sans Media Player avait été mis en place, et la concurrence rétablie[155]. Si la commission elle même reconnaît que « *la vente liée et l'intégration sont des pratiques fréquentes qui n'ont souvent aucune conséquence anti-concurrentielle* », [156]comment les entreprises du numériques peuvent-elles identifier les critères permettant de distinguer ce qui est légal de ce qui ne l'est pas ?

3. Une intervention du législateur centré sur la réglementation, justifiée par la théorie des infrastructures essentielles

Alors que les gouvernements ne sont pas aptes à se substituer au processus concurrentiel d'un marché libre pour garantir des services optimaux aux consommateurs, la position de la Commission Européenne reflète un durcissement de sa politique de concurrence qui n'est pas sans rapport avec l'agenda 2020. Or autant les Etats-Membres apparaissent divisés sur de nombreuses questions, en témoigne l'absence béante de pans entiers de problématiques relatives au numérique dans l'agenda 2020, autant nombre d'entre eux se préoccupent du comportement des GAFA, et ceci tant sur des questions de concurrence que sur des questions liées au traitement des données personnelles, à la fiscalité, ou encore au droit d'auteur et à la copie de contenus Web concurrents. Sur le plan de la concurrence, le

[155] Institut Economique Molinari « *La vente liée et l'intégration des produits nuisent elles aux consommateurs ?* » Mars 2006 p2-4
[156] DG Concurrence « Discussion paper on the application of Article 82 of the Treaty to exclusionary abuses » Décembre 2005 p. 54

Sénat Français à adopté le 15 avril 2015 l'amendement n°995 à la Loi Macron pouvant contraindre Google à donner aux utilisateurs le choix de trois moteurs de recherches concurrents sur sa version française. Le 3 janvier 2014, la formation restreinte de la CNIL a prononcé une sanction pécuniaire de 150 000 euros contre la Société Google. Inc. En l'espèce le G29, le groupe des CNIL Européennes, avait mené une analyse de la politique générale de confidentialité de Google qui depuis le 1er mars 2012, était la même pour l'ensemble de ses services (Google Search, YouTube, Gmail, Picasa, Google Drive, Google Docs, Google Maps), et avait constaté que celle-ci n'était pas conforme au cadre juridique européen. La CNIL a notamment considéré que « *la société n'informe pas suffisamment ses utilisateurs des conditions et finalités de traitement de leurs données personnelles* », qu'elle « *ne respecte pas les obligations qui lui incombent d'obtenir le consentement des utilisateurs préalablement au dépôt de cookies sur leurs terminaux* », et surtout qu'elle s'autorise, sans base légale, à procéder à la combinaison de l'intégralité des données qu'elle collecte sur les utilisateurs à travers l'ensemble de ses services. Ces conclusions de la CNIL sont les mêmes que celles qui ont été retenues par les autorités espagnoles et néerlandaises en 2013 au regard de leur droit national respectif.

Pour comprendre la position de l'Union Européenne, il convient d'expliquer la théorie des infrastructures essentielles, qui justifie en partie la stratégie économique de la Commission. Elle trouve sa source dans l'affaire Terminal Railroad Association tranchée par la Cour Suprême des Etats Unis d'Amérique en 1912[157]. Aux Etats-Unis, les procédures sont principalement ouvertes sur le fondement de la Section 2 du Sherman Act, qui exige la réunion de deux éléments complémentaires : « the possession of monopoly power » et «an anticompetitive conduct». Dans cette affaire, le Juge américain a consacré le principe d'intervention de la justice pour garantir l'accès à des facilités essentielles et garantir la concurrence dans le secteur ferroviaire. En Europe, la doctrine des facilitées essentielles a été énoncé de la façon suivante par le Professeur Temple Lang : « *if one competitor owns something, if access is essential to enable other competitors to do business, and if the competitors cannot be expected to provide this facility for themselves, the European Union competition law obliges the owner of the essential facility to give equal access to its*

[157] Cour Suprême des Etats-Unis, United States v. Terminal Railroad Association, 224 US 383, 1912.

competitors ».[158] Par conséquent d'après lui *«under this doctrine, the monopoly owner of an essential facility for competition may be forced to give access to that facility to competitors on reasonable and non-discriminatory terms*".[159] Cette théorie répond à l'impératif de garantir la concurrence sur un marché réunissant trois conditions : l'existence d'infrastructures essentielles, la position dominante du propriétaire de celles-ci, et l'abus de sa position dominante. Ces infrastructures sont des installations ou des équipements indispensables pour assurer la liaison avec les clients mais aussi pour permettre à des concurrents d'exercer leurs activités. Le propriétaire de la facilité dite « essentielle » voit donc ses droits de propriété restreints au profit des concurrents. L'Union Européenne a un champ d'application large de cette théorie, sur le base de l'article 102 du TUE sur l'abus de position dominante. Elle a été consacrée par l'affaire Sealink, la Commission a été saisie d'une plainte de l'entreprise SC le 15 avril 1993 au motif que Sealink aurait abusé de sa position dominante en tant que propriétaire et exploitant d'un port. La commission avait alors montré au point 57 de l'arrêt que « *l'exploitant d'une installation essentielle est tenu d'offrir un accès à des conditions non discriminatoires, la justification de mesures provisoires destinées à permettre à un nouveau concurrent d'accéder à un marché doit être beaucoup plus forte que dans le cas de mesures destinées à préserver la position d'un concurrent déjà établi.* »[160]. Si cet impératif ne contient pas de conditions spéciales d'application, la commission consacre ici l'obligation de considérer les infrastructures essentielles comme une entrave à la concurrence. Considérons le cas de Google par le prisme de la théorie des facilités essentielles. Cette entreprise dispose d'infrastructures essentielles puisqu'elle constitue le moteur de recherche le plus utilisé au monde avec 90,35 de parts de marché, devant Bing à 3,7% et Yahoo à 2,9%[161]. Or dans la communication de griefs visant Google, la DG Concurrence estime que l'entreprise a utilisé sa position dominante pour promouvoir son propre service Google Shopping au détriment de la concurrence. Elle justifie alors sa communication en invoquant le caractère incontournable du moteur de recherche Google ce qui constitue une réelle application de la théories des facilités essentielles, consacrées depuis la jurisprudence Sealink comme de véritables

[158] Temple Lang, John *«Defining legitimate competition: companies' duties to supply competitors and access to essential facilities»,* Fordham International Law Journal 1994, vol. 18, p 439

[159] Ibid

[160] Décision de la Commission Européenne, Affaire Sea Containers contre Stena Sealink, 21 décembre 1993, point 57

[161] Stat Counter Global Stats « Top 5 Desktop, Tablet & Console Browers from May 2015 to April 2016 »

plateformes pour l'ensemble de l'économie. Ce que pointe véritablement l'Institut Molinari, c'est l'utilisation du droit de la concurrence comme un instrument de la politique économique de l'Union Européenne. Or comme l'affirme le Professeur Louis Vogel « *la théorie économique, loin de n'être qu'une méthode à la disposition du droit dans le domaine de la concurrence, lui est consubstantielle. La théorie de la concurrence se trouve au fondement du droit de la concurrence: l'un ne saurait exister sans l'autre* »[162]. La théorie des facilités essentielles est donc parfaitement applicable au cas de Google, puisque son explication trouve ses fondements dans la théorie économique.

On peut cependant s'interroger sur la pertinence de l'arbitrage opéré par la Commission dans les affaires Microsoft et Google. Dans la première, la séparation des activités de vente liée ne s'est pas traduite pas une amélioration notable des conditions d'acquisition des consommateurs. Dans le deuxième cas, bien que la théorie des facilités essentielles permette de justifier l'intervention de la Commission, on peut réellement s'interroger sur la stratégie de celle-ci au vu du montant de l'amende qui pourrait être infligé à la firme de Moutain View dans les prochains mois, estimée à 3,1 milliards d'euros d'après The Telegraph[163]. Les GAFA, principaux collecteurs de données, se voient visées par une politique paradoxale de la Commission Européenne, qui tend d'une part à limiter la concentration de leurs activités pour laisser émerger des champions européennes, et d'autre part à harmoniser les législations des 28 Etats-Membres pour faciliter la circulation de ces données. Trop souvent, le marché intérieur du numérique et ses acteurs, se voient mis à l'épreuve. Il y a ici une double problématique puisque la politique concurrentielle de la Commission freine l'innovation, et l'harmonisation des législations laisse de côté un très grand nombre de sujets, entravant le potentiel du marché unique.

[162] Vogel, Louis « *Le juriste face à l'analyse économique* », ateliers de la Concurrence de la DGCCRF, 5 octobre 2012

[163] Williams, Christipher « *Google faces record-breaking for web search monopoly abuse* » Telegraph, 14 mai 2016

Conclusion :

A mon sens, les deux fils d'Ariane de ce mémoire, la question de la protection des données, et celle de l'influence du modèle américain sont intrinsèquement liées. En effet l'Union Européenne accuse aujourd'hui un regard considérable dans ce domaine. Alors que Washington dispose d'une expertise réelle, fondée sur une longue tradition datant de la mise en place de technostructures entre les entreprises de la Sillicon Valley et les services de surveillance américains après la chute du mur de Berlin, l'Europe peine à favoriser l'émergence de ses propres champions du numérique. Malgré l'influence des dispositifs d'autorégulation et des systèmes de gouvernance originaire des Etats-Unis, le législateur européen tente d'une part d'imposer une doctrine européenne de la protection des données, et d'autre part d'utiliser le bras armé de la DG concurrence pour limiter les possibilités d'action des GAFA. On peut réellement s'interroger sur la pertinence d'amendes aussi élevées et de choix de répression concurrentiels parfois dogmatiques de la part de Margaret Vestagher, qui privilégie parfois une vision court-termiste au détriment du consommateur. Le think-thank américain Cato Institute, critiquait déjà en 2001 la directive de 1995, estimant qu'elle n'était qu'une ficelle du dispositif protectionniste de l'Union Européenne appliqué contre les Etats-Unis pour favoriser ses entreprises.[164] Cette critique était justifiée à l'époque, la directive résultant moins d'une volonté de construire un régime de protection des données que d'un besoin d'harmonisation des politiques commerciales des Etats-Membres. Malgré les limites des possibilités d'action du législateur européen, conditionné à l'accord politique des Etats-Membres, il apparaît nécessaire que l'Union Européenne prenne la mesure de l'importance du numérique, en se dotant d'instances souples capables de prendre la mesure des changements dans ce secteur. En effet, un simple agenda destiné à accélérer la croissance et sécuriser la donnée ne suffira pas pour impulser un véritable changement. Pour impulser celui-ci, il est fondamental que l'Union Européenne recentre ses priorités autour de plusieurs axes.

Le premier, c'est une amélioration de la présence des Etats-Membres de l'Union dans les instances de gouvernance d'Internet. En effet, par le biais de l'ICANN, le département de commerce américain a aujourd'hui encore la mainmise sur la distribution des noms de domaines. L'Union Européenne doit inclure dans les négociations transatlantiques une

[164] Lukas, Aaron *« Safe Harbor or Stormy Waters ? Living with the EU data Protection Directive »*, Cato Institute, Washington, 2001

exigence d'indépendance pour l'ICANN qui de par sa nature et son monopole actuel, à vocation à être une agence des Nations Unies au même titre que l'Union Internationale des Télécommunications, l'ITU. Le deuxième axe qui doit être travaillé par l'Union Européenne, c'est la mise en avant de dispositifs d'autorégulation, favorables à l'émergence de nouvelles pépites européens du numérique, pour grossir le panel regroupant Blablacar, Shazam, Spotify et TransfertWise. Tout en permettant une sécurisation de la donnée, ces dispositifs devront favoriser la mise en place de véritables écosystèmes européens. En effet, jusqu'à présent les législateurs européens ont opposé à la privacy au copyright, et le droit à la vie privé au droit à la propriété de la donnée. Or, un rapport du Boston Consulting Group pointe la nécessité de rechercher un équilibre dans la réglementation, permettant à l'utilisateur de décider si il souhaite ou non partager ses données. En effet, la construction d'un régime juridique visant à protéger le consommateur peut retarder l'innovation dont ce même consommateur aurait pu bénéficier. [165] Ce paradoxe nous amène à une réelle interrogation : la technique peut-elle prendre le pas sur la norme démocratique lorsque les législateurs ne parviennent pas à l'encadrer sans freiner l'innovation ?

L'agenda numérique 2020, si il révèle une prise en compte réelle des enjeux juridiques entourant le marché intérieur du numérique, a été très critiqué par de nombreux acteurs et législateurs de ce marché. Lors d'un discours à l'Institut de droit comparé de Paris, Evelyn Ghebart, une des rares députés européennes à être spécialisée dans ces enjeux, à fait part de sa « déception » quant à l'agenda numérique, et a dénoncé l'absence de vues sur des sujets aussi importants que la lutte contre la cybercriminalité, la numérisation de l'industrie, et l'économie collaborative[166]. Elle pointe également le problème, que nous avons déjà abordé concernant les accords SWIFT, des différences de vues entre les deux institutions : un Parlement représentant les citoyens, et une Commission plus préoccupée par la recherche d'un accord politique entre les Etats-Membres. Concernant la donnée, ces différences de vues se traduisent par des tensions évidentes entre les intérêts commerciaux des Etats-Membres, qui souhaitent poursuivre les négociations transatlantiques, et l'inquiétude des citoyens européens, qui transparait dans le vote des résolutions des parlementaires. Alors que cette problématique ne peut être qu'appréhendée de manière à minima européenne puisque les activités sont par nature transfrontalières, ce sont les différences de conceptions entre les 28 Etats-Membres qui

[165] Boston Consulting Group « *The Value of our digital identity* » November 2012, p17-18
[166] Ghebart Evelyn, Discours au Forum annuel de Trans Europe Experts, 21 mars 2016

freinent pour l'instant la construction d'une doctrine européenne de la donnée,. Alors que la France souhaite par exemple la construction de ce régime sur des règles générales telles la transparence, la confiance et la protection des données, les deux tiers des Etats-Membres ne veulent pas entendre parler d'une telle éventualité[167]. A l'élaboration d'un édifice juridique temporaire et fragile, d'un règlement européen qui ne sera qu'un instrument anachronique dans deux décennies, ne devrions nous pas nous confronter à l'effrayante perspective de Lawrence Lessig : « *Code is Law, Law is Code* », en partant du postulat que la technologie ne doit être soumis à aucunes règles autres que celles qui assurent son fonctionnement ? La technologie Block Chain, véritable livre des comptes ouverts aux utilisateurs du monde entier qui annonce une destruction progressive des métiers du droit et de la banque nous amène à une véritable interrogation.

[167] Rogard, Pascal, Discours au Forum annuel de Trans Europe Experts, 21 mars 2016

Bibliographie :

I. Droit primaire

Textes de Droit Européen

Directives du Parlement Européen et du Conseil de l'Union Européenne :

- Parlement Européen et Conseil, Directive 95/46/EC relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données

Règlements du Conseil de l'Union Européenne :

- Conseil de l'Union Européenne, Dossier inter-institutionnel du Règlement UE 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation des données, abrogeant la directive 95/46/EC, 6 avril 2016
- Conseil de l'Union Européenne Règlement n°1/2003, article 11

Décisions du Parlement, du Conseil, et de la Commission

- Parlement Européen, Conseil, et Commission Accord InterInstitutionnel-« Mieux légiférer » (2003/C 321/01), 31 décembre 2003
- Décision de la Commission, relative à une procédure d'application de l'article 82 du Traité CE, du 24 mars 2004 (affaire COMP/C-3/37.792 Microsoft), JOUE, 6 février 2007, L 32/23.
- Décision de la Commission Européenne, relative à l'Affaire Sea Containers contre Stena Sealink, 21 décembre 1993

Résolutions du Conseil de l'Europe :

- Conseil de l'Europe, Comité des Ministres, résolution (73)22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, 26 septembre 1973
- Conseil de l'Europe, Comité des Ministres, résolution (74)29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, 20 septembre 1974

Résolutions du Parlement Européen

- Parlement Européen, Résolution sur la suspension de l'accord TFTP du fait de la surveillance exercée par l'agence nationale de sécurité américaine. 23 octobre 2013,
- Parlement Européen, Résolution 2015/2147 « Vers un acte sur le marché numérique », 19 janvier 2016

Documents de travail :

- DG Concurrence « Discussion paper on the application of Article 82 of the Treaty to exclusionary abuses » Décembre 2005

Textes de droit interne

Code Civil:

- Code Civil, Livre I, Titre I « Des droits civils », article 9

Décisions du Conseil Constitutionnel :

- Conseil Constitutionnel, Décision n°2010-45, QPC du 6 octobre 2010

Rapports de l'assemblée nationale :

- Assemblée Nationale, Commission des Affaires Européenne, Rapport n°4326 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère

personnel au sein de l'UE, notamment dans le cadre de la réforme de la directive 94/46/CE, 7 février 2012

- Assemblée Nationale, Rapport d'information n°3560 de M. Patrice Verchère, « Révolution numérique et droits de l'individu : pour un citoyen libre et informé » 22 juin 2011

Textes de droit américain

Sénat des Etats-Unis :

- US Senate, Juciary Committee, September 18, 2007 Statement for the Record to the House Judiciary Committee by Director John Michael McConnell
- US Senate, Foreign Intelligence Service Act (FISA), Title VII, Section 702 Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons"

Convention du département de commerce américain :

- National Telecomunication & Information Departement « Assessment of the Transition of the Technical Coordination and Management of the Internet's Domain Name and Addressing System » 24 avril 2009

II. Communications

Communications de la Commission Européenne:

- Commission Européenne, Communication « La Commission européenne présente le paquet «bouclier de protection des données UE-États-Unis» 29 février 2016
- Commission Européenne, Communication « Stratégie pour le marché unique numérique: la Commission européenne définit les grands domaines d'action » 25 mars 2015

- Commission Européenne, Communication « A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen » 6 mai 2015
- Commission Européenne, Communication « Pratiques anticoncurrentielles: la Commission adresse une communication des griefs concernant la prestation transfrontière de services de télévision payante disponibles au Royaume-Uni et en Irlande », 23 juillet 2015
- Commission Européenne, Communication « Unleashing the potential of Cloud Computing in Europe » 27 septembre 2012
- Communication de la Commission, « Abus de position dominante: la Commission adresse une communication des griefs à Google au sujet du service de comparaison de prix et ouvre une procédure formelle d'examen distincte concernant Android » 15 avril 2015
- Commission Européenne, Service juridique explication de l'arrêt T-201/04 Microsoft-abus de position dominante : « Concurrence-Microsoft-Abus de Position dominante » 17 septembre 2007

Communications de la CNIL :

- Falque-Pierrotin, Isabelle « Consensus sur le Paquet Européen Protection des données personnelles » Communication de la CNIL, 22 décembre 2015

Discours :

- Ghebart Evelyn, Discours au Forum annuel de Trans Europe Experts, 21 mars 2016
- Jucnker, Jean Claude « *Construire l'Europe industriel du numérique* » discours prononcé le 27 octobre 2015
- Thieulin Benoît, Discours du au forum annuel de Trans Europe Experts, 21 mars 2016
- Thieulin Benoît, Discours sur l'Europe du numérique à la Maison de l'Europe, 18 février 2016
- Rogard, Pascal, Discours au Forum annuel de Trans Europe Experts, 21 mars 2016
- Walter, Jean Philippe « *La convention 108-d'un standard européen vers un standard universel* ? » Exposé dans le cadre de la Conférence internationale sur la protection des données à Varsovie, 21 septembre 2011

III. Jurisprudences :

Jurisprudences de la CJUE :

- CJUE Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, affaire C-131/12, 13 mai 2015
- CJUE Bodil Lindqvist, affaire C-101/01 6 novembre 2003
- CJUE Satakunnan Markkinapörssi et Satamedia, affaire C-73/07, 16 décembre 2008
- CJUE, Affaires Jointes Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado, 24 novembre 2011
- CJUE arrêt Football Association Premier League Ltd et Karen Murphy, affaires jointes C-403-8 et C-429-8, 4 octobre 2011
- CJUE, Arrêt Hoffman-La Roche & Co.Ag contre Commission des Communautés Européennes 85/76, 13 février 1979

Jurisprudences de la CEDH :

- Cour Européenne des Droits de l'Homme, Vereinigung Bildender Künstler c. Autriche, 25 janvier 2007
- Cour Européenne des Droits de l'Homme, Vereinigung Bildender Künstler c. Autriche, 25 janvier 2007
- Cour Européenne des Droits de l'Homme, arrêt Muller contre Suisse, 24 mai 1988

Jurisprudences du TPICE :

- TPICE, Affaire T-201/04, Microsoft Corp. contre Commission des Communautés européennes, 17 septembre 2007
- TPICE, Arrêt dans l'affaire T-286/09 Intel Corp/ Commission, Communiqué de Presse n°82/14, 12 juin 2014

Jurisprudences du CE :

- Conseil d'Etat, arrêt d'assemblée M. Roujansky et autres, 23 novembre 1984

Jurisprudences de la Cour Suprême des Etats-Unis :

- Cour Suprême des Etats-Unis, United States v. Terminal Railroad Association, 224 US 383, 1912
- Cour Suprême des Etats-Unis, Sony Corporation vs. Universal City Studios Inc, 464 US 417, 1984.

IV. Traités Internationaux :

- Convention 108 du Conseil de l'Europe, 1er octobre 1985 « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »
- Convention européenne des droits de l'Homme, 4 novembre 1950, article 8
- Déclaration Universelle des droits de l'Homme, article 12, 10 décembre 1948
- Traité sur le Fonctionnement de l'Union Européenne, article 16, paragraphe 1 et 2
- Traité sur Fonctionnement de l'Union Européenne, article 26 paragraphe 2
- Traité sur le Fonctionnement de l'Union Européenne, articles 101 et 10

V. Articles et Ouvrages:

Articles institutionnels:

- CNIL, « Adoption du règlement européen par le Parlement Européen : un grand pas pour la protection des données en Europe » Article, 14 avril 2016
- Conseil Economique et Social « L'Etat actuel de la corégulation et de l'autorégulation dans le marché unique » Les cahiers du CESE, Février 2005

- Hustinx, Peter CEPD «*Le droit de l'Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données*», article CEPD, 14 septembre 2015
- Vie Publique « La DUDH de 1948 et la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950 »
- Vogel, Louis «*Le juriste face à l'analyse économique*», ateliers de la Concurrence de la DGCCRF, 5 octobre 2012

Articles universitaires :

- Brousseau, Eric « *Régulation de l'Internet :L'autorégulation nécessite-t-elle un cadre institutionnel* ? » Economie de l'Internet, Revue Economique, Numéro Spécial, Septembre 2001
- Cerf, Vinton et Khan, Robert « *« A protocol for packet network interconnection* » IEEE Transactions on Communications v.COM n. 5, Mai 1974
- Chatillon, Georges « *L'internet : bien public-bien privé-bien commun* » annuaire de le l'Université Paris I Panthéon Sorbonne
- Edouard Dubout et Alexandre Maitrot de la Motte «*L'Unité des libertés de circulation* », Bruylant, Septembre 2013, Avant Propos
- Holitsher, Marc « *Debate, Internet Governance* », La revue Suisse de la Science Politique n°5, 1999
- Johnson, Kevin, Martin, Scott, O'Donnell, Jayne and Winter, Michael« "Reports: NSA Siphons Data from 9 Major Net Firms". *USA Today*. , 15 juin 2013
- Joseph Vogel « *Comment apprécier les ventes liées en matière de droit la concurrence* », 14 avril 2010, Droit et Economie, Concurrences n°3-2°2010
- Klein, Hansel « *ICANN et la Gouvernance d'Internet, la coordination technique comme levier d'une politique publique mondiale* », Les Cahiers du numérique, 2002
- Manara, Cedric « *Le noms de domaines : fondation du droit de l'internet* » Power point sur le livre « *Les droit des noms de domaines* », 13 avril 2012
- Mueller, Mueller « *ICANN and Internet governance, sorting through de debris of self regulation* », INFO Vol 1, 6 Décembre 1999

- Poullet, Yves et Rouvroy, Antoinette « *Le droit à l'auto-determination informationelle et la valeur du développement personnel. Une révalutaion de l'importance de la vie privéé pour la démocratie* », Article de monographie, 2009
- Ramello, Giovanni « *Napster et la musique en ligne, le mythe du vase de Pandore se répéterait-il* ? » Hermès Sciences Publication, 2001
- Rotenberg, Marc « *Fair informations practices and the architecture of privacy* » Stanford Technologiy Law Revew, 2001
- Temple Lang, John «*Defining legitimate competition: companies' duties to supply competitors and access to essential facilities*», Fordham International Law Journal 1994, vol. 18
- Trudel, Pierre « *Quel droit et quel régulation dans le cyber-espace* ? », 2000 Sociologie et Société n°32
- Warren, Samuel et Brandeis, L « *The Right to Privacy* » Harvard Law Review N°5, Vol IV, 15 décembre 1890

Articles de presse :

- Anderson, Chris dans l'article de Guillaume, Hubert « *La gratuité est-elle l'avenir de l'économie ?* » Internet Actu, 10 mars 2008
- Boulet-Gercourt, Philippe *« Votre vie les intéresse »* Le Nouvel Observateur, 26 juillet 2001
- Caprioli, Eric *« L'Affaire Microsoft : concurrence versus innovation ? »* Journal du Net, 9 octobre 2007
- Dumontel, Fabienne « *Le droit à l'oubli numérique inquiète les historiens* », Le Monde, 3 octobre 2013
- Elyan, Jean *« Cloud computing : la commission européenne appelle à plus de normalisation »* Le Monde Informatique, 25 septembre 2012
- Gellman, Barton et Lindeman, Todd *« Inner workings of a top-secret spy program »,* The Washington Post, 1er juin 2013
- Guhman, Farid « *Face aux GAFA, l'Europe peut elle faire le poids ?* » Trop Libre, 5 novembre 2015
- Kallenborn, Gilbert « *La France a été la cible d'une cyber surveillance massive par la NSA* », Journal 01.net 1er juillet 2013

- Lacroix, Alexandre *« Faut-il avoir peur de la peur de la cyber-surveillance ?* » Philosophie Magazine, 20 septembre 2013
- Lausson, Julien « *Lawrence Lessig : couper l'accès à Internet, une idée terrible* » Numerama 21 novembre 2009
- Mousil, Marc *« Valeur sur le Net. Infomédiaires: les nouveaux champions du Web John Hagel et Marc Singer »* Alternatives Economiques n°185, octobre 2000
- Rolland, Sylvain 28 mai 2015 « *Comment l'Europe veut mettre les GAFA au pas » La Tribune*, 28 mai 2015
- Vandecasteele, Mylène « *L'économie des GAFA est maintenant aussi importante que celle du Danemark »* L'Express Business, 28 juillet 2015
- Vincent, Claude *«La ruée vers l'or des données personnels»*, Enjeux LesEchos, mars 2013
- Wilson, Matthew *« EU Commission open anti-trust case over geo-blocking »* Kitguru, 24 juillet 2015

Ouvrages *:*

- Anderson, Chris *« Webmail Windfal »* Wired 25 février 2008
- Babinet, Gilles « *L'ère numérique, un nouvel âge de l'humanité, cinq mutations qui vont bouleverser notre vie* » Broché, 23 janvier 2014
- Conseil de l'Europe et Agence des droits fondamentaux « *Manuel de Droit Européen en matière de protection des données* », avril 2014
- Farrell, Henry "*Constructing the International Foundations of E Commerce*." International Organization n°57 Printemps 2004 277–306, in « *The Global Governance of the Internet* (…) » of Daniel Drezner in 2002
- Godeluck, Solveig « *La géopolitique d'Internet* » La Découverte, août 2002
- Guillaume, Hubert *« La gratuité est-elle l'avenir de l'économie ? »* Internet Actu, 10 mars 2008
- Kemp, Simon « *The social traveller* », We are Social, 18 avril 2016
- Lessig, Lawrence « *L'avenir des idées : le sort des biens communs à l'heure des réseaux numérique* » Random House, 2001
- Lessig, Lawrence « *L'avenir des idées : le sort des biens communs à l'heure des réseaux numérique* » Broché, 1er septembre 2005 (traduction française)

- Rees, Marc « *Droit d'auteur, l'Europe veut s'attaquer au geoblocking* », Next Impact, 23 février 2015
- Rosenbaum, James « *In defense of the delete key* » The Green Bag, été 2000
- Sadin, Eric « *La vie algrothimique : critique de la raison numérique* » Broché, 12 mars 2015
- Williams, Christopher « *Google faces record-breaking for web search monopoly abuse »* Telegraph, 14 mai 2016

Articles think-thanks:

- Institut Economique Molinari *« Google versus Microsoft : du pareil au même ? »* 3 mai 2016
- Institut Economique Molinari *« La vente liée et l'intégration des produits nuisent elles aux consommateurs ? »* Mars 2006
- Lukas, Aaron *« Safe Harbor or Stormy Waters ? Living with the EU data Protection Directive »*, Cato Institute, Washington, 2001
- Vannini, Claire « *L'Affaire Microsoft : le droit de la concurrence saisi par le politique* », Fondation Robert Schuman, 19 novembre 2007

VI. Statistiques :

- Rapport Eurobaromètre 431, 8 juillet 2015
- Stat Counter Global Stats « Top 5 Desktop, Tablet & Console Browers from May 2015 to April 2016 »

VII. Autres :

- Andrus Ansip, « *Thanks for sharing your experience* » Twitt du 23 février 2015
- Boston Consulting Group « *The Value of our digital identity* » November 2012
- CIGREF « La réalité du Cloud dans les grandes entreprises » 9 octobre 2015

- Le blog du dirigeant, « *Cloud computing : définition, fonctionnement, avantages et inconvénients* », Image PNG
- Règlements de l'ICANN, Société de droit californien à but non lucratif, Article VI, Section 3 : critères de sélection pour les administrateurs

Annexes :

Annexe 1 : Veille législative et réglementaire sur la protection des données réalisée dans le cadre d'un stage au bureau européen de la Internet Society

Legislative and Regulatory Monitoring:

The necessity of a "European Digital Habeas Corpus"

« On the US NSA surveillance programme, surveillance bodies in various member states and their impact on EU citizen's fundamental rights and on transatlantic cooperation in Justice and Home Affairs."

Agenda:

1st of October 2013: The British MEP Claude Moraes published a draft report, claiming the necessity of a "European Digital Habeas Corpus". He resumed the period's debate by a single sentence: Is the situation created by Edward Snowden's revelations an indication of a general societal turn towards the acceptance of the death of privacy in return for security?" This non-official version was adopted with 33 votes for, 7 against, and 17 abstentions.

12 of October 2014 : The final report was adopted in Strasbourg with a large main. Indeed, the regulation passed with 621 votes in favour and the directive also passed with 371 in favour. This pack of text did respect most of the points the report presented in the LIBE

committee, with the notable exception of the Swift suspension (Society for Worldwide Interbank Financial Telecommunication) financial data.

15 of June 2015: The general approach to the regulation was decided by the Justice Ministers Council in order to start a Trilogue between the European Parliament, the European Council and the European Commission about a Data Protection reform.

24 of June 2015: The first Trilogue meeting took place around the commitment of the directive in the council, an agreement of the overall roadmap for Trilogue negotiations, and the definition of a general method and approach for delegated and implemented acts.

14 of July 2015: (still subject to agreement with Commission and Council) The second Trilogue meeting will take place around a precise draft agenda. The experts will begin by the subject of Territorial Scope (article 3) and International Transfers (Chapter V).

General Arguments:

On one hand, Snowden's revelations relate to US and some member's states intelligence services activities, and it's possible to consider that the EU has no competence in such matters. Moreover the argument of anti-terrorism necessity seems valuable: Edward Snowden denounces the inefficiency of the massive surveillance as a proper anti-terrorist measure, but anti-terrorism can still justify special policies. Another argument is that Snowden revelations remains an act of treason, and those revelations should be balanced against the need to preserve shared economic, business and foreign policy matters with the United States. Finally, as EU and US governments are democratically elected, they comply with democratic standards even when the intelligences services are, in the field of security, conducted to fight against terrorism.

On the other hand, the report record the references to Georges Orwell, saying that a focus on security and shift towards targeted and specific surveillance has seriously damaged and undermined the concept of privacy. Indeed, the concepts of privacy, data protection, freedom of press and fair trial are fundamental rights, currently threatened by surveillance measures and data retention. The other thing is that national security matters do not exclude EU

competence. Indeed, the EU has exercised the competences conferred upon it by the EU Treaties in matters of internal security by deciding on a number of legislative instruments and international agreements aimed at fighting serious crime and terrorism, on setting-up an internal security strategy and agencies working in this field. It's also important to remind that intelligence services, even if they insure an indispensable mission of security, do have the obligation to operate within the rule of law. Finally, the revelations of Edward Snowden have highlighted the pivotal role of the media when supervisory mechanisms fail to prevent or rectify mass surveillance.

Legal report:

The report presented 1sr of October 2013, after a remind of different acts, from the European Union and from the United States guarantying data protection, fundamental rights, surveillance and privacy issues, point out the anti-terrorism phase the world know since September 2001. The report point out the fact the progressive increase of mass surveillance measures which had not been subject to a prior debate about the place of such measures in a democratic system. Indeed, Edward Snowden revealed the existence of far-reaching, complex, and highly technology-advanced systems designed by the US and some member state's intelligence service to collect and store the citizen's data, all around the world. In order to protect European citizen's rights, the draft report shows different possibilities for the European Union. On the 12 of March 2014 a certain numbers of those possibilities were adopted in a final resolution (2013/2188 (INI).

About Member States Surveillance Services:

20. Calls on the US authorities and the EU Member States, where this is not yet the case, to **prohibit blanket mass surveillance activities**.

22. Calls on all EU Member States and in particular, with regard to its Resolution of 4 July 2013 and Inquiry Hearings, the United Kingdom, France, Germany, Sweden, the Netherlands and Poland to **ensure that their current or future legislative frameworks and oversight mechanisms governing the activities of intelligence agencies are in line with the standards of the European Convention on Human Rights and European Union data protection legislation** (…).

31. **Calls on the US to revise its legislation without delay in order to bring it into line with international law, to recognise the privacy and other rights of EU citizens**, to provide for judicial redress for EU citizens, to put rights of EU citizens on an equal footing with rights of US citizens, and to sign the Optional Protocol allowing for complaints by individuals under the ICCPR;

About International Transfers of Data and "Safe Harbour":

37. Considers that **large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour does not meet the criteria for derogation under 'national security'.**

38. Takes the view that, as under the current circumstances **the Safe Harbour principles do not provide adequate protection for EU citizens, these transfers should be carried out under other instruments**, such as contractual clauses or BCRs setting out specific safeguards and protections.

41. Calls on **Member States' competent authorities, in particular the data protection authorities, to make use of their existing powers and immediately suspend data flows to any organisation that has self-certified its adherence to the US Safe Harbour Principles**, and to require that such data flows are only carried out under other instruments and provided they contain the necessary safeguards and guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals;

54. Reiterates its resolution of 23 October 2013 and **asks the Commission for the suspension of the TFTP Agreement** (Terrorist Finance Tracking Program), which regulated the transfer of personal data.

74. Strongly emphasises, given the importance of the digital economy in the relationship and in the cause of rebuilding EU-US trust, that **the consent of the European Parliament to the final TTIP** (Transatlantic Trade and Investment Partnership) **agreement could be endangered as long as the blanket mass surveillance activities and the interception of communications in EU institutions and diplomatic representations are not completely abandoned and an adequate solution is found for the data privacy rights of EU citizens.**

European Strategy for cooperation and security:

57. Asks for an **immediate resumption of the negotiations with the US on the 'Umbrella Agreement', which should put rights for EU citizens on an equal footing with rights for US citizens** (…).

68. Calls on the Commission and the Member States to speed up **the work of establishing a European Cloud Partnership** while fully including civil society and the technical community, such as the Internet Engineering Task Force (IETF), and incorporating data protection aspects.

94. Calls on the Commission, standardisation bodies and ENISA to **develop, by December 2014, minimum security and privacy standards and guidelines for IT systems, networks and services, including cloud computing services, in order to better protect EU citizens' personal data and the integrity of all IT systems.**

Data Protection Reform:

60. **Calls on the Council Presidency and the Member States to accelerate their work on the whole Data Protection Package to allow for its adoption in 2014, so that EU citizens will be able to enjoy a high level of data protection in the very near future**; stresses that strong engagement and full support on the part of the Council are a necessary condition to demonstrate credibility and assertiveness towards third countries

61. **Stresses that both the Data Protection Regulation and the Data Protection Directive are necessary to protect the fundamental rights of individuals,** and that the two must therefore be treated as a package to be adopted simultaneously, in order to ensure that all data-processing activities in the EU provide a high level of protection in all circumstances (…).

63. **Considers higher transparency and safety standards for online and telecommunication as a necessary principle with a view to a better data protection regime**; calls, therefore, on the Commission to put forward a legislative proposal on standardised general terms and conditions for online and telecommunications services, and to mandate a supervisory body to monitor compliance with the general terms and conditions

Priority Plan:

132. **Decides to launch 'A European Digital Habeas Corpus - protecting fundamental rights in a digital age'** with the following actions: Adopt the Data protection Package, suspend the Safe Harbour and the TFTP, conclude the EU-US Umbrella agreement, evaluate agreements with third countries involving personal data, protect the rule of law and fundamental rights of EU citizens, develop a European Strategy for a greater IT independence, and finally develop the EU as a reference player for a democratic and neutral governance of the internet.

Political Groups reactions in the LIBE commission:

The LIBE commission finally adopted the report of the British MEP Claude Moraes on the 1st October of 2013 with 33 votes for, 7 against, and 17 abstentions**.**

The Green group/ALE found "scandalous" that it's amendment in order to offer a protection to Edward Snowden was rejected by the conservators and the social democrats, said Jan Philipp Albrecht.

The ALDE group, lead by Sophie in't Veld, reacted by saying how necessary it was to have democratic mechanisms to limit this surveillance, on the European level and on the National level.

The PPE group didn't publish any reaction following the adoption of this report, most of the conservators MP's chose the abstention.

The SPD group didn't' publish any reaction, most of the social democrats MEP's voted for the report.

Political Groups reactions after the final report adoption:

The European Parliament adopted the final version of the report on the 12 of March 2014. The regulation passed by 621 votes in favour, 10 against and 22 abstentions. The second element of the package, the directive, passed 371 votes in favour, 276 against and 30 abstentions.

If the regulation was the consensual part of Moraes report, **the conservative parties had announced they wouldn't approve the directive**. Timothy Kirkhope from ECR (European Conservatives and Reformists) wrote in a statement that he "cannot support this proposal as its overly prescriptive nature would prevent law enforcement officers from carrying out legitimate investigations."

The European Commissioner Cecila Malmström declared that she had the confirmation that the United States didn't collect the Swift data's, and, as a consequence, the TFTP agreement hadn't been violated. It might put in question the suspension of the SWIFT agreement.

Legislative consequences and Agenda:

European Commission:

Recently, the United States implemented a domestic reform of the Patriot act, voted on October 26, 2011 to extend law enforcement agencies' power for gathering domestic intelligence in the US. The recent suppression of the 215 article of the Patriot Act, which allowed security authorities to obtain tangible business records from companies under a secret judicial order with the vote of the Freedom act change the EU-US diplomatic relationship. According to the European Commission, it facilitates the negotiations on the other aspects as Safe Harbour, Swift or the TFTP. Concerning the TFTP, according to the DG Connect, it is out of question that it will lead top a regulation about Data Protection. Currently, the commission have to adopt an official position and is still negotiating with the United States on certain points like the "Safe Harbour". As a package of data protection based on the directive number 95/46 of the 24 of October 1995, the principle this agreement is as follow: An American company can certify the respect of European legislation, and in exchange is allowed to transfer personal data from the European Union to the United States.

European Council:

On the 15 of June 2015 the Council reached a general approach that allows the Parliament to establish a regulation on general data protection. Latvia's minister for justice Dzintars Rasnačs declare that she" salute the readiness of the European Parliament to start the trilogue negotiations already next week (24 of June 2015). Hopefully we will come to the final

agreement rapidly so that our citizens can enjoy the benefits of the reform as soon as possible". Those new data protection rights will be based around different notions: An easier access to the data, transparency and the use of a clear and plain language to inform citizens efficiently, a right of erasure of personal data and "to be forgotten" (recognised by the European Court of Justice in May 2014), the right of portability enabling easier transmission of the data from one service to another, and finally the limitation of the "profiling" use (automated asses of personal aspects of a personal data).

European Parliament:

Recently, on the 15 of June 2015, the European Parliament received the European Council's agreement to give the high common standards of data protection fit for the Digital Area. Jan Albrecht the Parliament's lead MP on the data protection regulation and Civil Liberties Committee Chair Claude Moraes both declared that they will work
towards finding a swift agreement on the Data Protection Regulation by the end of 2015 which will set out a "robust, modern, consistent and higher level of protection for the years to come".

European Data Protection Supervisor:

On the 4 of May 2015, the Supervisor Giovanni Buttarelli recalled the necessity to build "bridges for privacy protection. Bridges which are secure and dependable, in which citizens and business in our democracies can have confidence". He also called for a Data Protection reform based necessity, data minimisation, purpose limitation and transparency. He claimed that criticisms about Safe Harbour were justified, and explained the differences between the Safe Harbour and the EU-US umbrella agreement.

Conclusion:

The atmosphere of fear has influenced the European Union, mostly after the deadly attack on the French magazine *Charlie Hebdo***.** Currently, the whole problem about the balance between privacy and surveillance is the shift between the European treaties, conventions and declarations, and the reality faced by the national states in context of fear and mistrust. In the end of January, the Green Home Affairs Spokesperson Jan Philipp Albrecht commented the informal meeting on counter terrorism of the home ministers of Defence in Riga, saying:

“European governments and the EU are rightly focusing on what can be done to improve cooperation and prevent future terrorist attacks (…). Regrettably the misdirected focus on mass surveillance remains, with home affairs ministers renewing the push for a disproportionate air passenger data surveillance system.” Nowadays, the question is about the reform of Data protection rules, and the legislator’s capacity to make the balance between security and privacy. The recent adoption, on the 15 of June of a general approach to the regulation by the European Council is the first step of a long trilogue process in order to conclude the data protection package on December 2015.

Annexe 2 : Synthèse du Forum annuel de l'association Trans-Europe Experts

Réseau Trans-Europe Experts : création d'un vivier d'experts en 2009 sur les questions juridiques européennes. Participation à l'élaboration des textes, avec le Parlement Européen et la commission Européenne. Le 16 mai 2010, le DG de la DG Connect donnait le chiffre de 415 milliards d'euros, avec un cadre réglementaire et l'assurance d'une société numérique inclusive.

I. L'agenda numérique 2020 : Alain Lamassoure : « *Quelle politique fiscale face aux géants du numérique* ? »

Les vagues successives :

Première vague : Dans le domaine de l'information et de la communication autour des années 80. Multiplication des moyens de calculs d'une part. Loi de Moor (créateur d'INTEL) tous les 18 mois la capacité de calcul des ordinateurs est multiplié par deux.
Deuxième vague : Internet apparaissant en même temps que le PC. Puis Smartphone, permettant à tout le monde d'accéder à toutes les informations.
Troisième vague : L'extension des DATA à tout le monde devient ce qu'on appelle le Big Data. C'est la combinaison avec la connexion de tous les réseaux, de tous les ordinateurs et les micro-processeurs.

Pour les politiques, c'est un monde qui s'écroule, un monde et qui laisse place à une nouvelle économie. En France on a l'habitude que l'état soit à l'origine de tous les changements, ici ce n'est pas le cas ! C'est aussi un bouleversement pour les relations entre les générations. La vie politique elle même est bouleversée, puisqu'elle s'organise avec la société civile. Sans cette révolution technologique, pas de printemps arabe, pas de Daesh, pas de Bataclan, pas de progrès démocratique en Afrique. On a également une révolution de la médecine qui devient prédictive : tous les systèmes d'assurance vont être bouleversées.

Quelques-uns des concepts fondamentaux sont profondément bouleversés :

- A partir du moment où des besoins aussi fondamentaux que le besoin d'être logé ou véhiculé peuvent être satisfaits sans être propriétaire (airbnb/blablacar) ? Est-ce que la valeur de la propriété va demeurer ?

- Est-ce que le droit de chacun de nous de s'assurer de l'utilisation de ses données passe par un droit de propriété ou un droit d'usage ?
- Les entreprises du net se substituent au droit national, l'état est dépossédé au profit de nouveaux régulateurs mondiaux comme l'ICANN.
- La valeur ajouté : les plateformes AIRBNB aux Etats-Unis assurent plus de nuités que la totalité des entreprises américaines.
- La notion de Service Public : Les entreprises du numérique sont de fabuleux services publics de taille mondiale. Si Google avait été Français, on l'aurait nationalisé ! On a donc besoin qu'un certain nombre de règles s'inspirant du SP soit appliquées à ces entreprises.

La taxation de ces entreprises :

Au commencement était Luxleaks, a la suite des révélations d'un lanceur d'alerte, on consortium international de journalistes publient le dossier fiscal d'un grand nombre d'entreprises. C'est un cas phénoménal, non pas de fraude fiscal, mais d'évasion fiscale au Luxembourg. Ce sujet est apparemment comme simple, compréhensible par tout le monde, et scandaleux. Hors un grand nombre de députés souhaitaient appliquer aux entreprises le même système que pour la TVA. Jusqu'à présent 28 définitions différentes du bénéfice ! Il faut harmoniser cette définition. Chacun des états est donc le paradis fiscal de quelqu'un dans un domaine : pour le cinéma, il faut aller en France, en Belgique ou en République Tchèque. Il y a donc un eu appui des politiques et des législateurs sur ce scandale avec un double objectif :

Faire accepter par les 28 ministres des finances la compétence de l'UE et l'adoption de la même définition du bénéfice imposable, et au niveau planétaire, se mettre d'accord sur des règles de bases. Une entreprise doit payer ses impôts là où elle a son activité (CF jurisprudence entreprise néerlandaise contre Allemagne). Quels sont les critères ? Le CA, les bénéfices, le siège etc ? Qu'est ce qui définit l'activité ? CA effectif et bénéfice.

La bonne nouvelle, c'est que ça va marcher. La folie de sous fiscalisation pré-Luxleaks a fait que aujourd'hui plus aucun état ne peut se permettre de revendiquer officiellement la possibilité de revendiquer des avantages. Le secret bancaire, c'est terminé ! L'UE passe des accords avec Gernesey, la Suisse etc. Au delà, il y a un réel échange sur les données fiscales dans le monde : on aura accès à toutes les données financières de Facebook. La deuxième chose, c'est la publication au grand public de ces données chiffrées. Ca s'applique déjà aux banques puis l'année dernière, et ça s'appliquera sûrement aux géants du numériques.

Enfin les multinationales se rendent compte que le temps des ruses fiscales est terminé. Les entreprises vont pouvoir se concurrencer en étant des acteurs civiques modèles. Après le Bataclan, Zuckerberg invoque le drapeau français : des milliers d'internautes lui réponde, « Merci mais le meilleur moyen de contribuer à la relève de la France est d'y payer ses impôts ». Les Etats-Unis réagissent, ce qui permet à l'UE d'associer les américains à cet esprit. Ce problème est particulièrement aigue sur les entreprises digitales. Dans le cas du numérique, comment définir la valeur ajoutée ?

- Les données qu'on donne gratuitement à ces entreprises sont compensés par l'extraordinaire somme d'informations présente sur Google, Wikipédia etc. **On est à la fois consommateur et produit.**

II. L'agenda numérique 2020 peut-il permettre à l'UE d'affronter la révolution numérique :

Introduction : Après l'emploi et la croissance, Juncker a défini l'Europe du numérique comme la deuxième priorité l'agenda. On a 315 millions d'européens connectés mais seulement 7% des entreprises utilisant la vente en ligne, et 15% des consommateurs achetant en ligne. C'est un discours qu'on entend depuis les années 2000, et pourtant le marché ne décolle pas. Pourquoi ?

Discours de Pascal Rogard Diplomate en charge du numérique à la Représentation Permanante de la France auprès de l'UE: La commission Juncker a choisi le commissaire Oettinger qui n'a pas une très bonne réputation à Bruxelles, c'est significatif L'exportation

des PME transfrontalières traditionnelles est très peu développée. Le numérique étant un environnement naissant, on est encore dans la phase de gestation. Elle ne peut être appréhendée que de manière a minima européenne, puisque les activités sont par nature transfrontalière. Lorsqu'on achète sur Amazon on ne sait pas très bien d'où vient le produit. Les plateformes aujourd'hui ne sont qu'à 20% de leur potentiel de développement. Pour déréguler il faut une juridiction pouvant appliquer ces règles, mais comment les définir ? Comment réguler Google sans comprendre son algorithme de 250 critères ? La position de la France c'est de poser des règles générales, transparence, confiance, protection des donnés. Or 2/3 des pays européens ne veulent pas en entendre parler.

Discours de Evelyne Gebhardt, Député Européenne: Le Parlement Européen avait demandé depuis 2011 à la commission de se pencher sur ces questions. J'ai été déçu par l'agenda qui met de côté un grand nombre de problèmes, avec un manque énorme de vue globale des thèmes à voir : la cybercriminalité, la robotique et surtout l'économie collaborative. Se pose l'énorme problème des droits des citoyens. On a fait un premier pas avec une résolution votée le 19 janvier 2016, où on met le point sur certains thèmes importants, avec notamment le géo-blocking injustifié. Voulons nous avoir une commercialisation des données personnelles ? Un deuxième pan qu'on ne retrouve pas c'est la numérisation dans l'Industrie. Avec le système 3D on va avoir la possibilité de poser des problèmes à l'avenir. Le rôle du Parlement c'est de représenter les citoyens, et en ce qui concerne les Etats-Unis la commission européenne doit faire ce que les EM lui demande. Le Parlement a fait passer plusieurs résolutions contre ces négociations.

Jean Quatremer, Journaliste, Libération : Le commissaire n'est pas à la hauteur. L'agenda numérique est juste énumération de ce que va faire la commission. La question des droits d'auteurs : la commission fait comme si ça n'existait pas. La force de l'Europe alors qu'on a loupé la révolution numérique, c'est de produire le pétrole qui va dans les tuyaux. Les 28 états ont tous des conceptions différentes du droit d'auteur. La protection des données est une plaisanterie : la commission nous balance le bouclier américain remettant en cause cette protection des données. Elle n'arrive pas à son approche « marché » des 20 dernières années, il faut refaire de l'interventionnisme, **de *la politique industrielle***. La seule avancée concrète c'est la remise en cause du géo-blocking. En 1993, Jacques Delors avais sorti son livre blanc sur le numérique : et les EM n'avaient pas suivies. Les EM ont tous une seule préoccupation : céder aux américains. Seule l'Allemagne et le Parlement Européen font ça. Si la commission

se montrait plus dure, elle serait seule dans son combat. Nos états à cause du terrorisme, ont réussit l'exploit d'adopter, la France en tête un « Patriot Act » à la Française, alors que la commission refusait de le faire !

Carole Ulmer, Economiste, Confrontation Europe : Je partage une déception de l'agenda numérique européen. Tout n'est pas dans l'agenda, il y a des initiatives sur les compétences digitales, une discussion en cours sur la digitalisation de l'industrie. La bataille des plateformes est perdue, mais pourquoi ne pas préparer l'après Google !! En France on a de belles pépites : quoi de mieux qu'un marché européen du numérique pour créer ces écosystèmes dynamiques ? Il y a un début de réflexion sur le sujet aux Etats-Unis, avec un cadre de réglementation basé sur ces valeurs.

Benoît Thieulin, Président Conseil National du Numérique :

- Le dossier transatlantique a été un exercice d'archéologie, puisque les négociations étaient assez peu transparentes. Attention à ce que l'Europe en négociant ne troque pas un peu de notre présent voir notre passé pour notre avenir. Le SAFE HARBOUR concentre beaucoup des problématiques. Il a été négocié en 2000 par des gens ayant une vision très claire de la donnée et de son utilisation. Quelle est la manière dont se sont penchées ces gens ? Il y a une réelle asymétrie des questions stratégiques. Comment les américains avaient mis en place une réelle stratégie du numérique, et une politique industrielle (Voir conférence Confrontation Europe). Tout le monde comprend que c'est un phénomène générale de transformation. Même si l'arrivée de la commission Juncker : le CNUM a été entendu sur la portabilité des données.

- Nos élites ne maîtrisent pas le numérique ! A Washington, les conseillers ont tous autour de 35 à 40 ans. Ceux qui écrivent la feuille de route d'Obama, ce sont des anciens de Google, Facebook, et Microsoft. On doit faire la même chose.

- Comment faire dégager un IG européen ? Chaque mois perdu c'est des entreprises et de l'innovation en moins ! La commission disait que quand bien même ils aurait une feuille de route, comme mettre d'accord les 28 EM sur le sujet ?! Il y a une asymétrie de réflexion et de rapport de force.

- L’Europe est le plus grand marché unique numérique au monde. Les externalités positives sont gigantesques, mais l’essentiel est capté par les américains qui capte un aspect non négligeable sans pour autant payer. Le numérique n’est pas une révolution technologique, mais une révolution techno-culturelle (comme l’imprimerie). Cette chose là dessine les contours d’une autre civilisation dans laquelle l’Europe a son mot à dire. Il y a de quoi construire un modèle européen.

La neutralité du net ne marche que sur ses tuyaux. Le principe de ces plateformes c’est de ne pas être neutre. On a plutôt évoqué la loyauté. On doit donc inscrire dans le droit de nouvelles formes de régulation. On a poussé à la création d’une agence d’évaluation des plateformes et Le droit de la concurrence est complétement muet sur ce sujet. Les agences de notations expertes doivent participer ?

Philippe Dewost, Directeur en charge de l’économie numérique à la Caisse des Dépôts : Rapport sur les quartiers naissance donnant naissance à la French Tech de Fleur Pellerin. On avait relevé plusieurs paradoxes :

- Le premier est temporel : l’objet de départ va se trouver de plus en plus en décalage avec l’état du monde. Comme ça va très vite, il ne faut pas jeter la pierre au commissaire du numérique. La plupart des législateurs sont structurellement déconnectées.
- Le deuxième est géographique : d’un côté internet est partout, de l’autre il y a un aspect très local à l’investissement ! Comment répondre à la compétition sur laquelle Londres prend un temps d’avance sur nous. Il faut accepter l’émergence de l’imprévue. L’idée même du politique de dire qu’on a pas la main est impossible. Il faut offrir aux startups pus que le cadre législatif et fiscale sera stable sur la durée d’investissement, à savoir sur 7 à 10 ans. Si les règles du jeux ne sont pas stables, il est normal que les investisseurs soient frileux. Saint Exupéry : « L’avenir tu n’as pas à le prévoir mais à le permettre ».

L’AFC anglaise a choisi une approche intelligente : ils disent par un rapport : « on sait qu’il va falloir réguler, via une mécanique de consensus délocalisé » le fait d’engager la Block Chain peut être une solution.

Synthèse du débat :

- L’économie des communs n’a pas du tout été traitée par l’agenda numérique, qui n’est pas complet sur bien d’autres questions : la robotique, l’économie collaborative.
- Code is Law, Law is Code. La technique peut-elle prendre le pas sur la norme démocratique du fait de l’ignorance des législateurs ?
- Il faut protéger nos valeurs, sans trop nuire à nos entreprises.