Deuxième partie – L'Europe face aux défis de la « balkanisation »

La question des risques et des opportunités de la « balkanisation » pour l'Europe pose d'abord la question de ses objectifs qui ne semblent pas se dessiner clairement à ce jour. La tentation d'un repli souverain se fait de plus en plus forte au sein de l'UE et de ses Etats-membres, notamment depuis les révélations d'Edward Snowden. Les propositions en ce sens fleurissent et comportent des risques de fragmentation alors que les ambitions affichées en termes de puissance économique et de diffusion de ses valeurs requièrent à l'inverse d'être dans une dynamique d'ouverture.

L'UE est tiraillée entre deux tendances contradictoires ; entre la volonté de sanctuariser le territoire dans le but de protéger la souveraineté —qui recèle aussi des bénéfices économiques pour les entreprises de sécurité nationales— et les nombreux enjeux de développement économique à l'échelle globale. Même si le terme de « balkanisation » est également repris en Europe, il reste employé avec beaucoup de circonspection à cause de la tentation de repli souverain qui s'opère dans de nombreux pays européens.

1 Les enjeux politiques et économiques

Les révélations d'Edward Snowden ont mis en lumière la complexité des enjeux qui se posent pour l'UE. Alors que l'Europe était désignée comme « une colonie du monde numérique » dans le rapport Morin-Desailly du printemps 2013, l'UE (Commission et Parlement) a assez vivement réagi aux annonces de la surveillance de masse orchestrée par la NSA : réaction diplomatique, ouverture d'une enquête sur « la surveillance massive des citoyens de l'UE », menaces sur les accords Safe Harbor et TTIP, etc. Le principal enjeu pour l'UE est de sortir de cet état de « colonie du monde numérique » pour s'émanciper, sur le plan politique, de l'extra-territorialité pratiquée par les Etats-Unis et sur le plan économique et industriel de la suprématie américaine, et tenter de donner une impulsion au marché européen (création d'emploi, croissance économique, relocalisation fiscale) voire créer les conditions nécessaires à la création de nouvelles opportunités. Il s'agit dès lors de permettre l'émergence d'industriels européens sans toutefois restreindre le marché au seul marché européen. Mais si les enjeux politiques et économiques sont importants, ils sont en fait intimement liés aux enjeux de sécurité et de souveraineté.

1.1 Des réalités disparates au sein de l'UE en matière numérique

Le premier enjeu pour l'Europe est certainement celui de la disparité des situations en matière de numérique au sein de l'UE. Le manque d'uniformité au niveau européen sur un certains nombres de points comme la question du marché du numérique ou encore la fiscalité constitue la première difficulté pour l'Europe afin de faire bloc face aux défis de la balkanisation et notamment dans le domaine économique. Un marché européen fragmenté ne peut faire le poids face aux géants américains.

La réduction de la fragmentation du marché du numérique en Europe est identifiée comme l'un des objectifs principaux de la stratégie numérique de l'Union européenne définie en 2010. Mais la mise en œuvre d'un marché unique numérique peine à se concrétiser, comme en témoigne le discours de Neelie Kroes, Commissaire au numérique, d'octobre 2013 appelant les acteurs à s'atteler à la formation de ce marché[113]. Ainsi, alors même que depuis l'affaire Snowden, le contexte politique pourrait se prêter plus facilement à l'instauration d'un tel marché, il semble que des blocages persistent. Il s'avère que le manque d'uniformité réglementaire et normative constitue une véritable barrière pour les utilisateurs, les industriels, les opérateurs et les entreprises les cantonnant principalement à leurs marchés nationaux[114]. La mise en conformité avec un ensemble important de législation au sein de l'UE constitue un véritable frein pour les PME innovantes dans ce domaine qui ne parviennent pas à exporter leurs produits et à pénétrer de nouveaux marchés en Europe.

Stéphane Grumbach et Stéphane Frénot estiment que « *les Etats européens ont fait l'impasse, ou tout au moins ont échoué à promouvoir les entreprises de la nouvelle économie* » [115]. Les deux chercheurs expliquent cet état de fait par la difficulté politique de mettre en place les outils de traitement et d'exploitation des données en Europe notamment pour des raisons historiques propres à l'Europe. Les Etats européens craignent un détournement des données personnelles des citoyens comme ce fut le cas lors de la Seconde Guerre Mondiale. En France notamment, la loi en vigueur (directive de 95) limite strictement la collecte des données. Grumbach et Frénot considère ainsi qu' « *en ne construisant pas*

[113] Source : http://europa.eu/rapid/press-release_SPEECH-13-787_en.htm
[114] Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions, *Une stratégie numérique pour l'Europe : faire du numérique un moteur de la croissance européenne*, Bruxelles, 18 décembre 2012
[115] Article Grumbach et Frénot Hérodote

d'industrie du Web2.0, l'Europe s'est privée de l'accès à la ressource y compris à la ressource provenant de ses territoires »[116].

Or l'UE a fait du numérique l'un des piliers de ses objectifs en termes de croissance et de compétitivité : « *La croissance durable et la compétitivité future de l'Europe reposent, dans une large mesure, sur sa capacité à embrasser la révolution numérique dans toute sa complexité. Les technologies de l'information et de la communication sont de plus en plus présentes dans tous les secteurs de la société et de l'économie et on estime que les investissements dans les TIC sont à l'origine de tous les gains de productivité réalisés* »[117]. A ce jour, force est de constater que les pays de l'UE ne sont pas égaux dans le développement du numérique. Selon une communication de la Commission Européenne[118], il faudra notamment faire face à un déficit de compétence numérique. Une étude estime en effet qu'un million d'emplois hautement qualifiés dans le domaine des TIC ne seront pas pourvus d'ici à 2015[119].

En outre, les Etats-membres de l'UE doivent faire face à un autre manque d'uniformité à l'origine d'une importante concurrence entre les Etats européens : la fiscalité. On observe en effet que les géants du web sont principalement domiciliés en Europe dans les Etats aux taux de TVA les plus faibles ; et notamment l'Irlande qui bénéficie de l'un des impôts sur les sociétés les plus bas en Europe[120]. Les géants du web dont Apple ou encore Facebook ont su tirer parti de la concurrence fiscale entre les Etats-membres de l'UE. Par exemple, pour l'exercice 2012, Google a déclaré avoir réalisé un chiffre d'affaires de 193 millions d'euros pour ses activités en France, mais n'aurait payé que 6,5 millions d'impôts sur les sociétés. Or son chiffre d'affaire réel réalisé en France est estimé pour 2011 entre 1,2 et 1,4 milliards d'euros[121]. Au début de l'année 2014, ils ont été suivis de Yahoo! qui a annoncé que les activités du groupe en Europe seraient désormais concentrées et gérées depuis Dublin alors que l'entreprise avait jusque là fait le choix d'une territorialisation de ses services. Ce manque d'uniformisation engendre une inadéquation certaine entre les revenus générés par les géants du web au sein des différents Etats-membres de l'UE et leurs taux d'imposition respectifs. En

[116] Grumbach S. et Frénot S., « Les données sociales, objets de toutes les convoitises », *Hérodote*, n°152_153
[117] Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions, *Une stratégie numérique pour l'Europe : faire du numérique un moteur de la croissance européenne*, Bruxelles, 18 décembre 2012
[118] Source : http://europa.eu/rapid/press-release_MEMO-14-383_en.htm
[119] Etude de suivi des compétences numériques, *eSkills Monitor*, Commission européenne, 2009
[120] Center for European Economic Research, *Effective Tax Levels unsig the Devereux / Griffith Methodology*, 2012, p.5
[121] http://www.franceinfo.fr/emission/le-vrai-du-faux/2013-2014/le-vrai-du-faux-du-13-06-2014-06-13-2014-07-25

2012, Plusieurs rapports en France notent le caractère profondément européen de cet enjeu d'harmonisation car « *les premières tentatives de création d'une fiscalité propre à l'économie numérique, effectuées dans un cadre strictement national, manquent leur cible* »[122].

1.2 Une Union européenne absente sur le plan industriel

Le premier constat est celui de l'absence d'une offre industrielle européenne dans le domaine de l'informatique de façon générale mais surtout dans le domaine du Big Data et de la cybersécurité. Or ces deux marchés, aujourd'hui dominés par les Etats-Unis, représentent des enjeux économiques et de sécurité majeurs pour l'ensemble de l'Union européenne. Dans ce contexte, les discours sur la protection des intérêts économiques et de sécurité de l'UE se sont développés. Ils se sont traduits dans plusieurs Etats-membres par des politiques de sanctuarisation de l'espace européen mais aussi des espaces nationaux, par exemple par la valorisation d'offres industrielles dites « souveraines ». Ces dynamiques industrielles ont pour effet de produire une fragmentation économique et réglementaire qui pourrait à terme servir de base à une fragmentation politique. Or ces évolutions vont à l'encontre des principes de l'accord de partenariat transatlantique de commerce et d'investissement (TTIP), actuellement en négociation, qui prévoient l'instauration d'une zone de libre échange entre les Etats-Unis et l'Union Européenne.

1.2.1 Sur le marché informatique

Sur le plan informatique de façon générale, une analyse complète sur la chaîne d'approvisionnement (systèmes d'exploitation, microprocesseurs, serveurs, etc.) n'a pas encore été menée pour les 28 pays de l'Union, mais plusieurs rapports nationaux ont fait l'état des lieux de la dépendance européenne vis-à-vis des fournisseurs provenant de pays tiers[123]. De fait l'offre quasi inexistante dans le domaine de l'informatique positionne l'UE dans une situation de dépendance vis-à-vis des fournisseurs étrangers et renforce ainsi sa vulnérabilité. Le tableau ci-dessous résume cette situation pour les quatre principaux segments du marché : informatique grands publics, informatique mobile, informatique de réseau et informatique d'automatisation. Le constat est clair : sur quasiment toute la chaîne de valeur, les entreprises

[122] Rapport Colin et Collin sur la fiscalité du numérique, p.3

[123] Voir notamment le rapport d'information « *L'Union européenne, colonie du monde numérique ?* » de la sénatrice française Mme Catherine MORIN-DESAILLY, fait au nom de la commission des affaires européennes n° 443 (2012-2013) - 20 mars 2013. Le Livre blanc rédigé par l'Association Française des Éditeurs de Logiciels et Solutions Internet, *Cyber-sécurité : Hisser les acteurs français au niveau de la compétition mondiale*, juin 2014. Ou encore le rapport du Department for Business, *Innovation and Skills (BIS) Impact Assessment of NIS Directive*, 2013.

non européennes se partagent les marchés. Cependant il existe une exception : les logiciels industriels, domaine dans lequel les entreprises européennes ont une longue tradition. Toutefois ces dernières ne sont pas présentes sur le segment sécurité du marché. Des investissements sur ce segment pourraient constituer l'opportunité pour les entreprises européennes de se positionner en acteur dominant du marché de la sécurité des logiciels industriels (voir partie 3).

L'affaire Snowden a montré à quel point l'industrie des TIC pouvait impacter le rapport de force géopolitique et stratégique entre les Etats. Les grandes entreprises américaines et asiatiques dominent toute la chaîne d'approvisionnement du cyberespace, de la couche physique jusqu'aux services : OS, composants électroniques, serveurs, applications (mail, navigateurs, etc.), moteurs de recherche, etc. Les Etats-Unis ont su mobiliser leur industrie et en tirer profit sans comparaison aucune avec ce qui existait jusqu'à présent. Cet avantage est déjà exploité à des fins de guerre économique[124]. Il constitue également un avantage précieux pour la collecte et l'exploitation des données, dont les retombées économiques sont majeures.

NIVEAU DEPENDANCE DE L'UNION EUROPEENNE DANS LE DOMAINE DE L'INFORMATIQUE[125]	
Totalement dépendante en informatique grand public	Informatique de bureau (PC) : pas d'offre européenne, domination des Etats-Unis (HP/Dell/Apple) et de l'Asie notamment la Chine (Taiwan/Lenovo)
	Processeurs graphiques (GPU) : pas d'offre européenne, offre 100% américaine (AMD/Intel/ Nvidia)
	Cartes-mères : marché dominé par Taiwan (Asus,

[124] Danilo D'Elia, « La guerre économique à l'ère du cyberespace », *Hérodote*, 2014/1 n° 152-153, p. 240-260.
[125] Les informations pour la compilation de ce tableau sont à trouver dans plusieurs études : « La cybersécurité Enjeux et perspectives d'un marché en pleine mutation », Xerfi, 2012 ; « Forecast: PCs, Ultramobiles, and Mobile Phones, Worldwide, 2010-2017, 4Q13 Update », Gartner, 2013, IC insights, Major 2013 IC Founderies, 2013 ; Marché des smartphones : Samsung n°1, Apple n°2 au Q3 2013 ~ IDC, Eco Conscient ; Industrial Control Systems (ICS) Security Market Market Forecast & Analysis (2013 - 2018), Market and Market, 2013 ; « La Cybersécurité Europeenne : de l'importance d'une politique industrielle », rapport de Jeremy Labarre, stagiaire ENA au Conseil de l'Union européenne, 2014

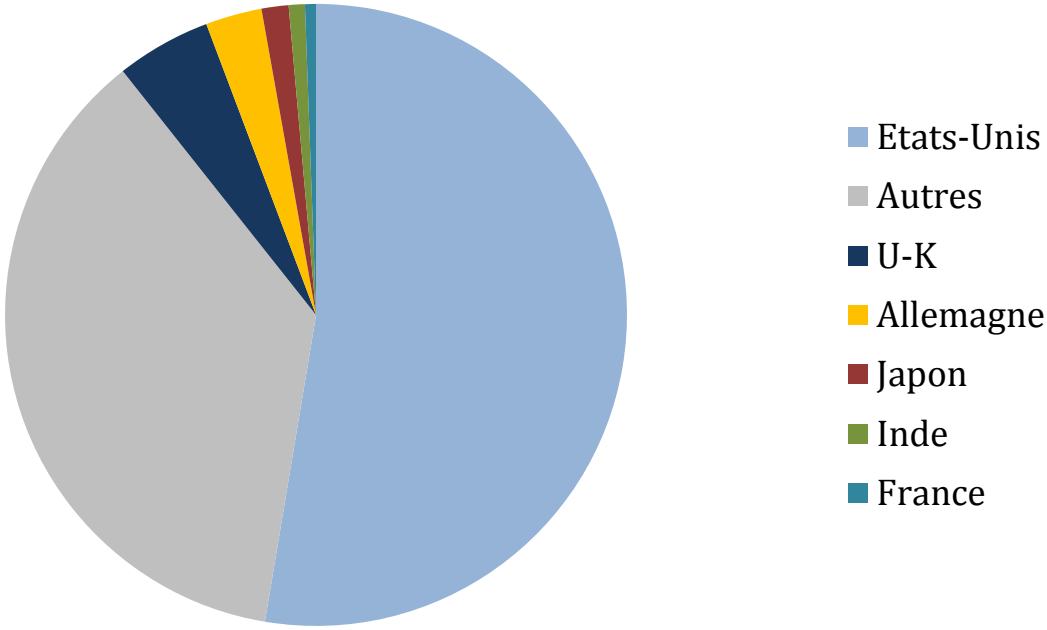
	Gigabyte, ASRock, Microstar International)
	Semi-conducteurs maitrisés dans la conception, la création des masques et les outils d'implantation (STMicrolectronics) mais l'Union européenne est dépendante à 100% de fonderies extra européennes.
Totalement dépendante en informatique mobile	Constructeurs de Smartphones : partagés entre coréens (Samsung, LG), américains (Apple/Microsoft) et chinois (Huawei, Lenovo)[126]
	Processeurs mobiles : partagés entre coréens (Samsung), américains (Qualcomm, Apple) Taiwan (Mediatek)
Très dépendant en informatique de réseau	Routeurs cœur de réseau : partagés entre Etats-Unis (CISCO, Juniper) et Chine (Huawei et ZTE)
	Commutateurs Ethernet : marché dominé par les Etats-Unis (CISCO, HP, Juniper, Dell) même si Alcatel Lucent possède une offre
	Serveurs informatiques : dominés par Etats-Unis (IBM, HP, Dell, Oracle, Cisco) et Japon (Fujitsu)
Satisfaisante en informatique d'automatisation	Logiciels de gestion de production assistée par ordinateur : 3/4 des leaders sont européens
	SCADA : 3/4 sont européens mais la production reste en Chine
	Automates programmables industriels (API) : dominé par une société américaine (Rockwell Automation) mais forte présence européenne (Schneider Electric et Siemens AG)

[126] Rappelons la chute de Nokia qui était un des leaders mondiaux avant d'être racheté par Microsoft

1.2.2 Sur le marché du Big Data

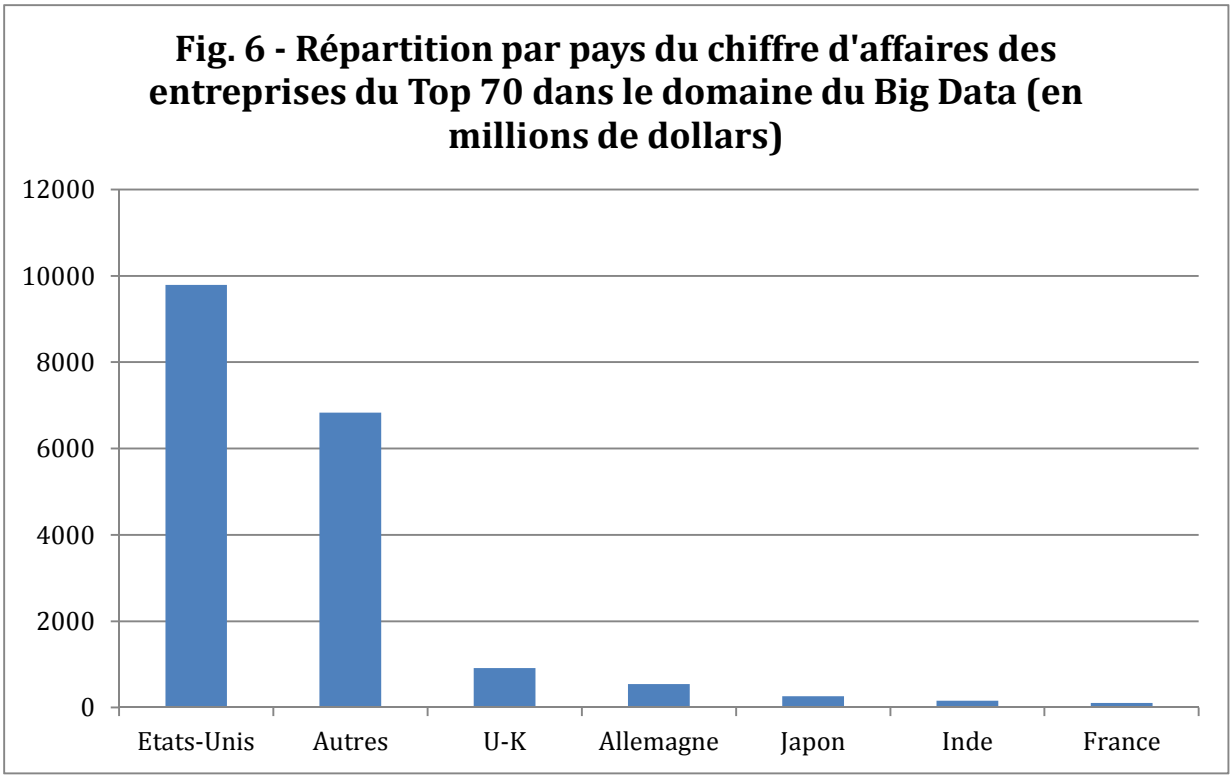
Le marché du Big Data est certainement l'un des enjeux économiques les plus importants dans le domaine du numérique. Les prévisions oscillent mais toutes prévoient des perspectives de croissance importantes. Le marché de 11,5 milliards de dollars en 2012 atteindrait presque les 50 milliards de dollars en 2017/2018[127]. Là encore l'Europe semble en retrait, voire nettement en retard. Pour Transparency Market Research, l'Amérique du nord concentre 55% du marché et selon leurs analyses cette domination va s'accroitre même si les auteurs notent l'émergence rapide de la région Asie-Pacifique dans le domaine[128]. Le top 70 des entreprises de Big Data montre d'ailleurs très clairement la suprématie des Etats-Unis.

Fig. 5 - Répartition du Top 70 des entreprises du Big Data par pays



[127] Big data Value, Framing a European Partneship for a Big Data Value Ecosystem, février 2014 Source : http://www.bigdatavalue.eu/index.php/downloads/finish/3-big-data-value/13-vision-for-a-european-big-data-value-partnership/0

[128] Transparency Market Research, Big Data Market – Global Scenario, Trends, Industry Analysis, Size, Share And Forecast 2012-2018,

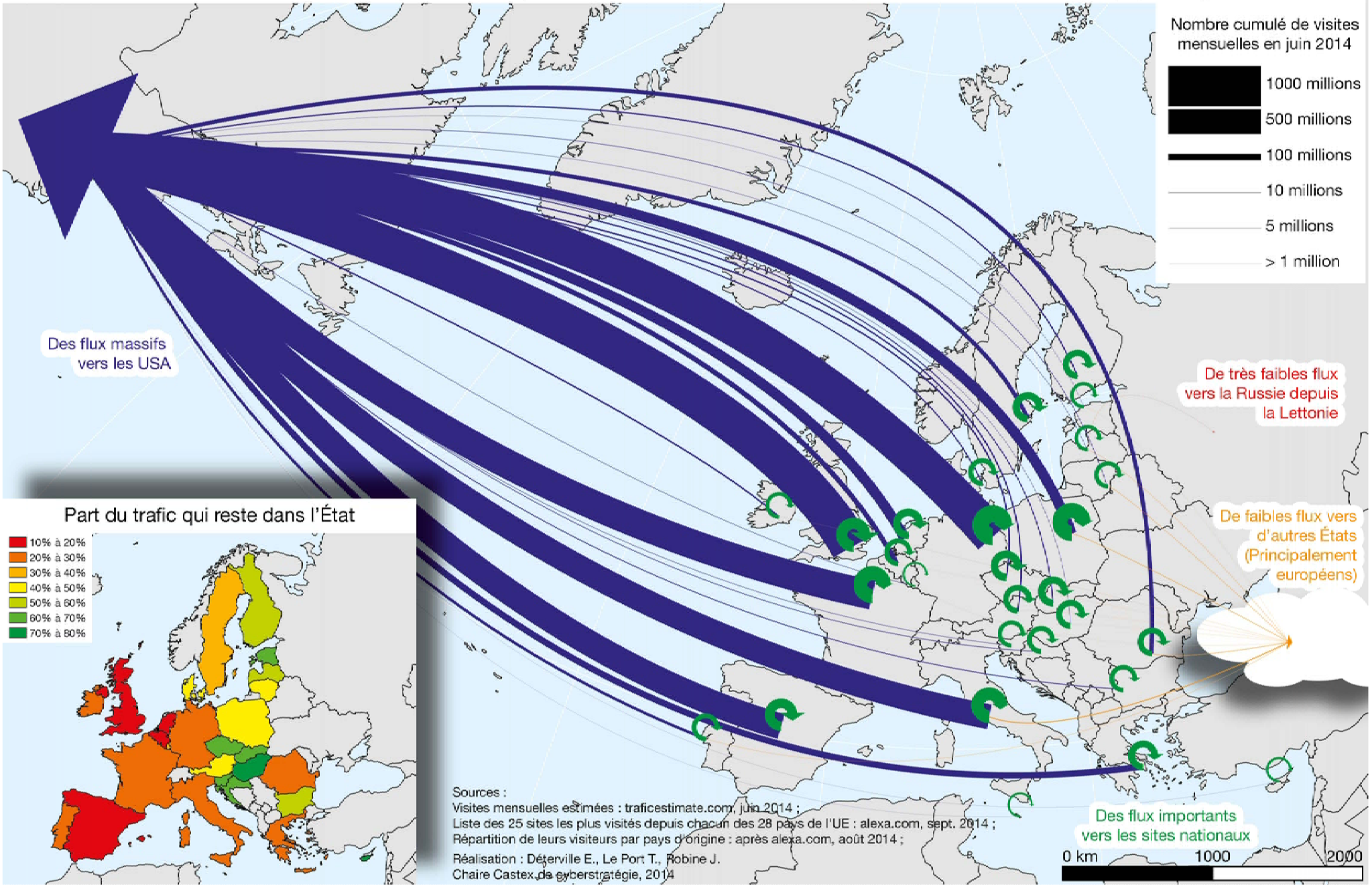


Source des Fig. 5 et 6 :
http://wikibon.org/wiki/v/Big_Data_Vendor_Revenue_and_Market_Forecast_2013-2017

La carte ci-dessous illustre la suprématie américaine en termes de captation des flux de données. On voit ici que les Etats-Unis sont le « grand aspirateur » de données. L'Europe n'y échappe pas, cependant parmi ces vingt-huit pays les écarts sont conséquents. Pour chaque pays une balance des flux entrants et sortants a été réalisée. Ainsi les pays d'Europe de l'Ouest sont bien plus déficitaires (rouge et orange sur la carte) que les pays de l'Europe de l'Est (en jaune et vert sur la carte). Cette carte a été réalisée à l'aide du Top 25 des sites internet les plus visités pendant un mois.

11. - Les flux de données en Europe, massivement captés par les États-Unis

Visites mensuelles estimées des 25 sites les plus visités depuis chacun des 28 pays de l'UE et répartition de leurs visiteurs par pays d'origine du site



Comparant les données à un nouvel or noir, Stéphane Grumbach et Stéphane Frénot expliquent que « *si des raisons géologiques expliquent la concentration des matières premières dans des régions particulières, des raisons économiques et politiques gouvernent leurs flux sur la planète. (…) La comparaison souvent faite avec le pétrole illustre parfaitement une caractéristique essentielle de l'économie des données personnelles : la concentration* »[129]. Dans ce cas, la localisation des données n'est pas fixée par des facteurs naturels mais par les concentrations économiques et les environnements règlementaires.

1.2.3 Sur le marché de la cybersécurité

Le marché de la cybersécurité représente un marché mondial de produits et services de forte innovation estimé à 50 milliards d'euros[130]. Ce marché nécessite des investissements en R&D constants afin de s'adapter aux évolutions permanentes des menaces et des technologies (en moyenne autour de 20% du chiffre d'affaire d'une entreprise)[131]. En outre, les cycles de développement et déploiement sont très courts (entre trois mois et trois ans) et se déploient à une échelle mondiale. Au cours des six dernières années, ce secteur a vécu des transformations profondes tant en termes de demande (+20% pour la période 2011-2014, secteur civil et militaire[132]) que d'offre (formation de *pure players*). Malgré la croissance de ce marché, qui devrait s'amplifier avec la prise de conscience des dirigeants d'entreprises encouragée par l'affaire Snowden, ce dynamisme masque des réalités inquiétantes pour l'Union européenne.

D'une part, les Etats-Unis captent la moitié du marché, avec 23 milliards d'euros alors que l'Europe ne représente que 12,5 milliards d'euros[133]. D'autre part, il existe une grande disparité au sein des pays européens car la France, l'Allemagne et le Royaume Uni totalisent à eux seuls entre 8 et 9 milliards d'euros de part de marché[134]. En effet, la demande en matière de cybersécurité demeure émergente à l'échelle européenne et n'est pas encore mature dans de nombreux Etats-membres, d'autant qu'il n'existe pas de politique industrielle européenne en la matière. Ajoutons à cela que les Etats-Unis ont investi massivement dans le domaine depuis une dizaine d'année (3 milliards de dollars par an seulement pour la R&D)[135].

[129] Article Grumbach et Frenot pour Hérodote
[130] Visiongain, *Global Cyber Seucrity Market Report 2013-2023*
[131] *Ibid.*
[132] *Ibid.*
[133] *Ibid.*
[134] *Ibid.*
[135] *Ibid.*

Ensuite, l'industrie européenne est extrêmement fragmentée, et quand les compétences existent, elles sont souvent méconnues ou sous capitalisées. Les start-up n'ont donc pas la possibilité de se développer en pérennisant leur R&D et sont insuffisamment protégées face à des stratégies de rachat agressives de la part d'entreprises étrangères et notamment américaines, comme on l'a observé lors du rachat de Stonesoft par McAfee. En fait, en dehors de niches ultra spécialisées comme la défense (BAE Systems, Airbus Defence and Space, Thales), qui sont en outre principalement tournées vers des marchés nationaux, les industriels européens n'ont pas encore développé une offre adaptée (large et à un prix compétitif) pour répondre aux besoins du secteur privé (entreprises et particuliers).

Le marché se structure de la façon suivante :

- *Business to Government* : Il s'agit d'un marché *high grade* et de niche. A l'exception des Etats-Unis, le volume est estimé entre 50 et 100 millions par an et par pays. Ce segment correspond aux marchés de cyberdéfense dans lequel les intégrateurs du secteur de la défense comme Lockheed Martin aux Etats-Unis ou Airbus et Thales en France et Grande-Bretagne jouent un rôle important. Les clients sont principalement les agences gouvernementales, les armées et les services de renseignement.
- *Business to Business :* Ce segment est qualifié de *mid grade*. La demande y est constituée par les grands opérateurs économiques avec de forts besoins de sécurité et de défense mais ne pouvant accéder au segment *high grade* car trop cher ou parce que les standards ne sont pas adaptés aux systèmes d'information commerciale.
- *Business to Customer* : Dans ce marché *low level* en termes de besoin de sécurité, l'achat est plutôt guidé par le rapport prix/performance et la réputation du fournisseur. Ce marché correspond en grande partie au marché des antivirus et des *firewalls*. Les géants américains dominent ce marché qui est déjà en deuxième phase de verticalisation ou aspiré dans la colonne des grands éditeurs de solutions d'infrastructure comme en témoigne la vague d'acquisition au cours de l'année 2010[136].

Le principal problème de l'Europe est qu'il n'existe pas encore d'écosystème cohérent d'entrepreneurs (grands groupes et PME), de laboratoires et d'investisseurs capables d'assurer

[136] Intel a racheté McAfee pour 5,7 milliards d'euros, HP a racheté ArcSight pour 1,1 milliard d'euros, ou encore Verisign qui a racheté Symantec pour 1 milliard d'euros).

une innovation continue et un socle technologique répondant aux enjeux sécuritaires et économiques que posent les cybermenaces. Ainsi, dans le top 20 des entreprises mondiales du secteur de la cybersécurité 14 sont américaines et 6 européennes. Alors que les compétences existent au sein même de l'Union européenne, notamment au sein de PME, ces dernières peinent à acquérir une taille critique pour devenir des entreprises de taille intermédiaire (ETI) et ainsi être capables de résister à la compétition[137]. La question de la taille du marché européen répond en partie à cette problématique. En effet, le marché unique du numérique n'est pas encore en vigueur et les PME se positionnent souvent sur le seul marché national, trop petit pour leur permettre de se développer. Ensuite, les programmes de recherche et les dispositifs de financements, comme le programme Horizon 2020[138], sont certes efficaces mais ne sont pas spécifiquement tournés vers le développement de solutions industrielles. En effet, il n'y a pas la capacité d'exécution pour faire de la recherche un succès commercial et en tirer des gains économiques (compétitivité, emplois). A titre d'exemple, 5% du marché mondial en 2013 a été généré par des entreprises israéliennes qui sont de dimension comparable aux entreprises françaises, mais qui bénéficient d'un système bien rodé en termes de financement et de coopération entre pouvoirs publics et industriels. Les entreprises européennes peinent alors à attirer des investisseurs en capital risque, et ainsi à se développer.

Au moment où les prévisions de marché à l'export sont évaluées à +30%,[139] la défaillance d'une industrie européenne se traduit par une perte de compétitivité de la base industrielle européenne au profit des grands groupes étrangers, particulièrement américains, sur les marchés externes. En interne, le marché est laissé aux compétiteurs étrangers qui profitent du coup d'un effet pervers de la directive NIS.

Ce rapide état des lieux de la situation en Europe permet de dresser une liste des principaux enjeux pour l'UE en matière de politiques économiques et industrielles. Le constat sévère dressé par ce tableau montre toute la marge de manœuvre et de progression de l'Europe sur ces questions.

[137] Elles ont souvent un chiffre d'affaires ne dépassant pas les 5/10 millions.
[138] Le programme Horizon 2020 est un programme européen pour la recherche et le développement pour la période 2014-2020
[139] Déclaration d'un représentant de l'ANSSI lors d'une conférence organisée le 7 mai 2014

1.3 Se protéger contre l'extra-territorialité de la législation américaine : vers des politiques de *data localization* ?

Plusieurs exemples ont montré combien la législation américaine permettait aux Etats-Unis de capter et de mobiliser un grand nombre de données collectées et stockées par les grands opérateurs américains. Les compétences extraterritoriales de la législation américaine constituent un véritable enjeu pour l'Union européenne en matière de protection de ses citoyens et bien sûr de souveraineté. Cette dynamique recouvre également des enjeux économiques, notamment l'émergence d'une offre européenne en matière informatique et de cybersécurité. Cependant dans un monde post-Snowden, les dynamiques ont tendance à évoluer comme le montre le cas récent de Microsoft qui a, pour l'instant, refusé de fournir à la justice américaine l'accès à des données hébergées sur le sol européen (en Irlande) malgré la demande d'un juge fédéral mais la procédure est toujours en cours. L'extra-territorialité de la législation américaine représente un coût sécuritaire pour l'UE mais aussi un coût économique. La localisation des données est ainsi devenue un enjeu important au sein des Etats-membres qui y voient une opportunité de protéger les données de leurs citoyens et de leurs entreprises de la surveillance des Etats-Unis.

Les entreprises américaines ont également été éclaboussées lors des révélations d'Edward Snowden, notamment en termes de confiance de leurs clients autres qu'américains, le tout dans un contexte où les offres *cloud* prennent de plus en plus d'importance. Le marché européen constitue un véritable enjeu pour l'industrie américaine en matière de services numériques. En outre, pour le domaine du *cloud computing*, l'industrie américaine pourrait perdre entre 21,5 et 35 milliards de dollars pour les trois prochaines années à cause de la perte de confiance des acteurs européens selon un *think tank* américain[140]. S'il est à ce jour difficile de mesurer l'impact économique des révélations d'Edward Snowden sur les géants de l'informatique et du web, il est néanmoins possible de constater que leurs récentes stratégies témoignent d'une crainte de voir les entreprises et acteurs européens fuir leur offre de biens et services. L'Allemagne a par exemple déjà écarté Verizon de l'un de ses marchés publics au profit de l'opérateur national Deutsche Telekom pointant la défiance du gouvernement allemand vis-à-vis de la firme américaine ; même si la branche locale de Verizon proclamait dans un communiqué que « *Verizon Allemagne est une entreprise allemande et nous nous conformons aux lois allemandes. Le gouvernement américain ne peut pas accéder aux*

[140] Daniel Castro, « How Much will PRISM Cost the U.S. Cloud Computing Industry? », Information Technology and Innovation Foundation, août 2013. Source : http://www2.itif.org/2013-cloud-computing-costs.pdf

informations clients localisées en dehors des Etats-Unis »[141]. Pour les géants américains, le risque de perdre des marchés semble réel en Europe mais également en Asie où le gouvernement chinois a pris le même type de décisions en écartant de ses marchés publics Apple, Microsoft ou encore Cisco[142].

Le refus de coopération de Microsoft avec la justice américaine témoigne parfaitement des nouvelles stratégies développées par les entreprises américaines. Alors que la justice fédérale américaine réclame à l'entreprise américaine de lui donner accès à des informations dans le cadre d'une enquête, Microsoft refuse au motif que ces données sont hébergées sur un serveur en dehors des Etats-Unis. Pour le géant américain ce refus s'inscrit dans la volonté dans le but de prouver à ses clients à travers le monde, mais particulièrement européens, que leurs offres de biens et services servent et protègent leurs clients plutôt que le gouvernement américain. Ce bras de fer pourrait remonter jusqu'à la Cour Suprême des Etats-Unis.

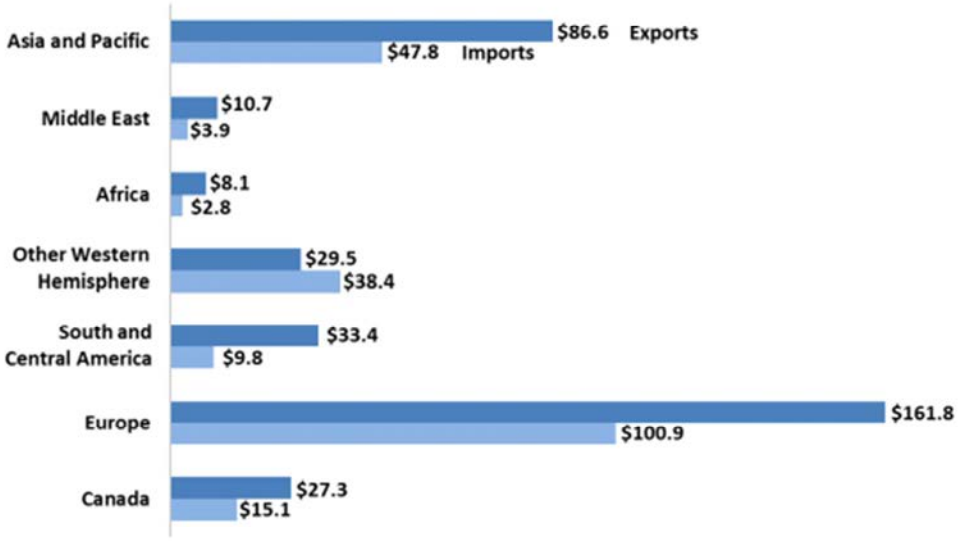
Cette problématique de la confiance des clients des géants du web américains est particulièrement importante dans le contexte du développement du *cloud computing*, que nous étudierons plus loin. Il est tout à fait plausible de voir ce type d'initiatives se multiplier, d'autant plus que ces mêmes entreprises (Apple, Cisco, Microsoft, AT&T ou encore Verizon) ont demandé, tout comme l'Electronic Frontier Foundation, une réforme du système de surveillance américain[143]. Leur demande évoque cinq principes à respecter[144] :

- Limiter la capacité des autorités gouvernementales dans la collecte des informations des utilisateurs ;
- Etablir un cadre légal clair pour la collecte et la compilation des données par les agences de renseignement ;
- Instaurer davantage de transparence dans les demandes d'informations des utilisateurs par les gouvernements auprès des entreprises ;
- Respecter la libre circulation des flux d'information et ne pas contraindre les FAI à localiser leur infrastructure dans un pays ou d'opérer localement;
- Eviter les conflits entre les gouvernements en développant un cadre pour traiter des demandes légales entres différentes juridictions sur le modèle des *Mutual Legal Assistance Treaties*.

[141] Source : http://www.lemondeinformatique.fr/actualites/lire-scandale-de-la-nsa-le-gouvernement-allemand-ne-veut-plus-de-verizon-57943.html
[142] Source : http://www.reuters.com/article/2014/06/04/us-china-usa-tech-idUSKBN0EF0CA20140604
[143] C'est une position intéressante de la part des entreprises car jusqu'à présent elles n'étaient pas connues pour leur position sur la vie privée ou la surveillance.
[144] Source : https://www.reformgovernmentsurveillance.com/

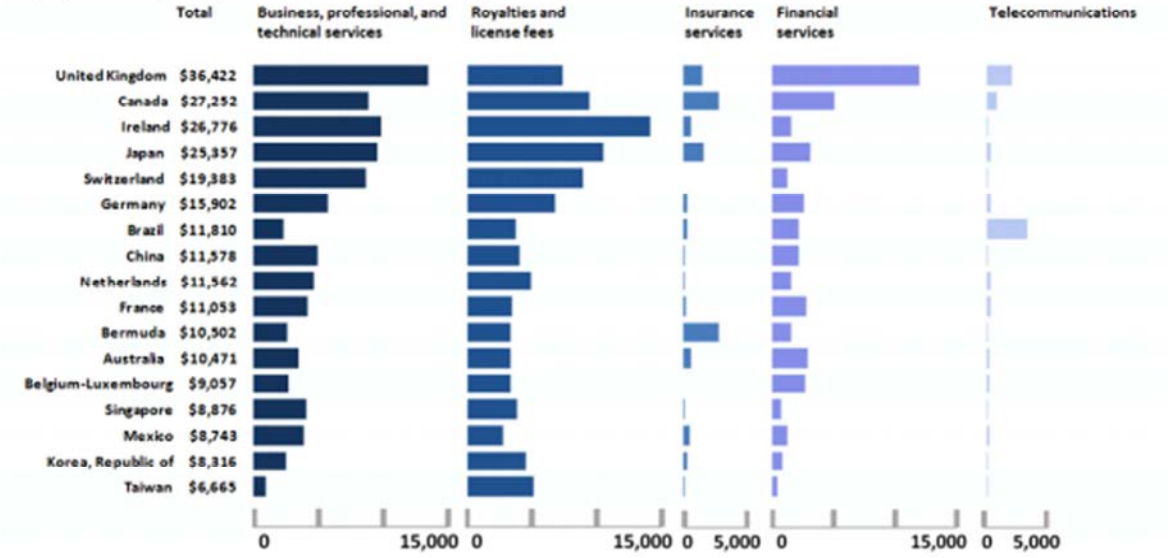
Pour ces entreprises, le marché européen n'est pas sans importance. Rien que pour les services numériques, l'Europe représente plus de 161 milliards de dollars des exportations américaines en 2011 selon une étude du département du Commerce américain[145]. L'Europe constitue à ce titre le premier marché en termes d'exportations des services numériques pour les Etats-Unis. Elle constitue également en 2011 le premier marché en termes d'importations.

Fig. 7 - Exportations et importations américaines de services numériques, par régions ou pays de destination ou d'origine en 2011 (en milliards de dollars)



Source: Economics and Statistics Administration analysis using data from the Bureau of Economic Analysis (BEA).
Note: Region definitions can be found on the BEAwebsite at:
http://www.bea.gov/international/bp_web/geographic_area_definitions.cfm.

Fig. 8 - Exportation américaines de services numériques par catégories et pays d'origine (en millions de dollars)



Note: Data on exports of insurance services to Belgium-Luxembourg and Switzerland are suppressed to avoid disclosure of data of individual companies.
Source: Economics and Statistics Administration analysis using data from the Bureau of Economic Analysis

[145] J. Nicholson et R. Noonan, 2014, Digital Economy and Cross Border Trade : The Value of Digitally-Delivrable Services, US Department of Commerce, Economics and Statistics Administration, p.12

Afin de répondre à ces enjeux, l'Union européenne et les Etats membres développent des stratégies de *data localization* principalement dans le but d'imposer aux entreprises d'héberger les données des citoyens européens sur le sol européen. C'est notamment le cas du projet de *Data Protection Regulation*, aussi nommé du nom de son rapporteur Jan Philipp Albrecht, qui a été adopté en première lecture au Parlement européen le 12 mars 2014. On peut également citer les projets de *cloud* européen et français étudiés plus loin dans ce rapport. En juin 2013, la Secrétaire d'Etat à l'Economie Numérique expliquait que la localisation des *« datacenters et serveurs sur le territoire national pour assurer la sécurité des données* » était un élément primordial alors que le projet de *cloud* français était lancé depuis l'année 2012 [146]. Comme en témoigne la déclaration de la Secrétaire d'Etat à l'Economie Numérique française, l'ensemble de ces initiatives est valorisé par les gouvernements européens comme une réponse aux enjeux sécuritaires mais est également mise en avant comme une solution aux enjeux économiques.

Conçues dans le but de favoriser l'émergence d'une industrie européenne, ces initiatives ont également pour objectif de profiter à la croissance et à l'emploi au sein des Etats-membres et de la zone UE, comme le pointe l'intégralité des documents issus de la Commission européenne sur le sujet. Cependant, il existe des divergences sur ces aspects.

Des études issues du Département du Commerce américain ou de la Chambre de Commerce américaine américaines montrent à l'inverse que l'impact des politiques de *data localisation* serait limité voire totalement fictif. Selon ces études, elles auraient pour effet de restreindre le marché en renforçant la concentration des activités entre les mains des acteurs les plus importants qui auront les moyens de s'adapter aux différentes réglementations. Ainsi, in fine ces politiques pourraient avoir un effet contre-productif par rapport aux objectifs de départ en accentuant le pouvoir des acteurs les plus importants qui sont aujourd'hui américains. Selon une étude de l'European Centre for International Political Economy, un *think tank*[147] à Bruxelles, commandée par l'U.S. Chamber of Commerce, la suspension du *Safe Harbor*, qui permet aux entreprises américaines ayant obtenu la certification de transférer les données de personnes de l'espace économique européen vers les Etats-Unis, engendrerait une chute du PIB de l'UE entre -0,8 et -1,3%. En outre, les exportations de services européens aux Etats-Unis pourraient chuter jusqu'à 6,7% à cause de la perte de

[146] Source : http://www.latribune.fr/technos-medias/informatique/20121002trib000722485/cloud-a-la-francaise-fleur-pellerin-justifie-les-deux-projets-concurrents.html
[147] Un lobby dont Google fait partie

compétitivité engendrée[148]. Pour certains auteurs citant ces mêmes études, les dynamiques de *data localization* répondraient davantage à des objectifs servant des intérêts au delà des buts affichés en matière de lutte contre la surveillance : anti-américanisme, protectionnisme mais aussi la volonté de développer la surveillance nationale.

Sur le volet relevant davantage des enjeux de sécurité, plusieurs experts s'interrogent sur les questions de la localisation des données. Une étude du cabinet Gartner souligne en effet que la localisation physique des données n'importe finalement pas autant que les discours peuvent le laisser penser. En réalité, en mettant en avant la complexité des questions numériques et du jeu des relations entre les différents acteurs impliqués, l'étude met en évidence qu'il faut davantage être attentif à la « localisation logique » des données, à savoir délimiter qui a accès aux données. L'étude montre même que la localisation physique des données est finalement d'importante relative car elle ne supprimerait pas les enjeux de sécurité posés. En effet, selon Gartner, la localisation physique ne suffirait pas à garantir que les données ne soient pas exploitées par les Etats-Unis et en particulier leurs services de renseignement, surtout si les données sont hébergées auprès d'un des géants du secteurs, qui, comme on l'a vu précédemment, sont majoritairement voire quasi exclusivement américains. Les législations à vocation extraterritoriale des Etats-Unis ne permettent pas d'assurer la sécurité et la protection des données en hébergeant simplement les données sur un territoire autre qu'américain[149]. Ainsi, la « localisation légale » des données constitue un enjeu bien plus important que la simple localisation physique; et ce d'autant plus que les services d'hébergement sont souvent sous-traités par une seconde entité. C'est ainsi que le Brésil, au cours de l'élaboration du *Marco Civil da Internet*, est revenu sur un amendement qui imposait aux entreprises de stocker les données de citoyens brésiliens sur le sol brésilien[150], en optant finalement pour une approche légale à savoir que toutes les opérations de collecte, stockage, rétention ou traitement sur des données personnelles devront respecter la loi brésilienne sur la protection de la vie privée[151]. Le cabinet Gartner distingue un dernier type de localisation à prendre en considération. La « localisation politique » dépend des risques politiques liés au territoire d'hébergement des données en fonction des dynamiques de coopérations

[148] European Centre for International Political Economy, « The Economic Importance of Getting Data Protection Right : Protecting Privacy, Transmitting Data, Moving Commerce », Mars 2014 Source : https://www.uschamber.com/sites/default/files/legacy/grc/020508_EconomicImportance_Final_Revised_lr.pdf
[149] En tout cas pour l'instant en attendant la décision de justice dans l'affaire de Microsoft sur les données en Irlande.
[150] Geetha Hariharan, *Marci Civil da Internet : Brazil's 'Internet Constitution'*, The Center for Internet and Society, 3 avril 2014 http://cis-india.org/internet-governance/blog/marco-civil-da-internet
[151] Article 11 du Marco Civil da Internet (Loi n°12.965 du 23 avril 2014).

internationales. Même si la tendance qui semble se dégager est que les géants sont moins enclins à coopérer avec la justice américaine lorsque les données ne sont pas hébergées sur le territoire américain, il peut toujours exister des moyens plus coercitifs pour les autorités américaines.

Par ailleurs, l'accord *Safe Harbor* signé entre la Commission Européenne et le Département du Commerce des Etats-Unis, offre un cadre juridique aux entreprises américaines certifiées (par le G29) pour transférer les données personnelles des citoyens européens vers les Etats-Unis dans le respect de la directive européenne 95/46/CE entrée en vigueur en 1998. De manière symbolique, le jour de l'adoption en première lecture du rapport Albretch, le Parlement européen adoptait également le rapport d'enquête sur la surveillance électronique de masse. Ce rapport préconise la suspension du cadre *Safe Harbor* auprès de la Commission ainsi que le rejet du Traité de libre-échange transatlantique en cours de négociation, le TTIP. Il appelle en outre à l'instauration d'un « *habeas corpus* numérique ». Le cadre *Safe Harbor* est remis en question non seulement sur des bases politiques mais aussi légales. A la suite de la plainte d'un autrichien, Maximilian Schrems, à l'encontre du siège de Facebook pour l'Europe, basé en Irlande, la Cour de Justice de l'Union européenne (CJUE) a été saisie et invitée à se prononcer sur la validité du cadre *Safe Harbor*.

Dénoncées comme un risque de fragmentation et une menace pour l'intégrité et l'unicité de l'Internet dans un certain nombre de publications américaines, les initiatives procèdent avant tout d'un rééquilibrage d'un rapport de force jusque là favorables aux Etats-Unis. L'ensemble de ces initiatives et stratégies constitue ainsi une volonté des Etats européens de mettre fin à la suprématie de la législation américaine.

Cet exemple de la *data localization* montre combien les débats sont plus complexes qu'il n'y paraît car elle revêt en fait une diversité d'approches et soulèvent de nombreuses questions afin de développer les stratégies les plus efficaces et non les plus simplistes.

1.4 Le respect des valeurs de l'Europe : rayonner sur la scène internationale

1.4.1 Pour l'instauration d'un régime de protection des données à caractère personnel protecteur

Le respect de la vie privée et la protection des données personnelles sont garantis par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Ces articles

précisent notamment que le respect à la vie privée vaut pour les communications (art.7) et qu'en matière de protection des données à caractère personnel, « *ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi* »[152] (art. 8). Ainsi l'Union européenne dispose d'un cadre légal portant des valeurs en adéquation avec la mise en place d'un régime de protection de données personnelles équilibré pour les citoyens européens. De plus, les principes de l'Internet tels qu'énoncés dans la première partie de ce travail, sont également largement compatibles avec les valeurs européennes affirmées dans le traité sur l'Union européenne. En effet, celui-ci dispose que : « *l'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'état de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités. Ces valeurs sont communes aux Etats membres dans une société caractérisée par le pluralisme, la non discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes* ».

Selon un sondage Eurobaromètre en 2013, 37% des Européens craignent de voir leurs données à caractère personnel utilisées à mauvais escient par un tiers, soit une diminution de 3 points par rapport à 2012[153]. Si le résultat peut paraître étonnant, c'est parce que le sondage a été réalisé du 24 mai au 9 juin soit juste avant et peu après les premières révélations d'Edward Snowden[154]. Il y a fort à parier que les résultats du prochain Eurobaromètre seront plus élevés après une année de révélations qui aura contribué à la sensibilisation de l'opinion publique sur cette question.

Pour l'Europe, l'enjeu est d'une grande importance. Il s'agit de mettre en place un cadre efficace et cohérent économiquement de protection des données à caractère personnel au sein de l'UE. L'arrêt de la Cour de Justice de l'Union Européenne (CJUE) Google Spain c/ AEPD du 13 mai 2014 stipule que, selon la directive n° 95/46/CE, les moteurs de recherche sont responsables du traitement des données personnelles sur les individus[155].

La décision de la CJUE s'inscrit dans les réflexions en matière de droit à l'oubli, qui devrait être plutôt qualifié de « droit au déréférencement », a contraint Google à proposer à

[152] Article 8 de la Charte des droits fondamentaux de l'Union européenne
[153] Special Eurobarometer 404, Cyberserity Report, Novembre 2013
[154] Les premières révélations publiées sur la base des documents de d'Edward Snowden interviennent le 6 juin 2013.
[155] Arrêt de la cour de justice de l'Union Européenne du 13 mai 2014 dans l'affaire Google Spain c/ AEPD Source : http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=264183

ses utilisateurs européens un formulaire en ligne dédié ; un exemple suivi par Bing et bientôt par Ask.com et Yahoo !. Cet exemple illustre que l'Union européenne peut imposer aux géants du web, décrits jusque-là comme tout-puissants, le respect d'un cadre juridique et des valeurs européennes (au moins pour les internautes européens pour l'instant). Si le modèle fonctionne, d'autres Etats pourront être enclins à adopter le même type de cadre juridique qui protégera leurs citoyens. Il reste que cette décision a soulevé des questions majeures. Google l'a annoncé dans plusieurs communiqués de presse, l'afflux de requêtes est considérable. Début juillet, le géant annonçait qu'il avait reçu 70 000 demandes en seulement un mois[156]. Leur traitement demande ainsi à la firme de Mountain View, une mobilisation de moyens humains et financiers. Mais plus encore, cette décision de la CJUE pose la question de l'arbitrage de ces demandes et de ce que certains ont appelé « le droit de savoir » (en opposition au droit à l'oubli). Certains acteurs (en particulier les médias britanniques) ont en effet avancé l'argument selon lequel cette décision constituait une porte ouverte à la censure mettant ainsi en avant les différences de conception de vie privée entre le monde anglo-saxon et le reste des Européens. Comme évoqué dans la première partie, la question de la responsabilité de Google dans l'arbitrage de ce qui doit être déréférencé ou non constitue un débat important. Il reste en effet de nombreuses questions sur les procédures à inventer. A ce titre, Google a mis en place un groupe de travail qui a organisé en septembre 2014 des réunions publiques sur cette question de l'équilibre entre le respect à la vie privée et la liberté de l'information[157]. En outre, la question du déréférencement sur les différentes versions de Google fait débat parmi les spécialistes et est en lien avec les enjeux de la multiplicité des juridictions. Aujourd'hui la firme de Mountain View effectue ses déréférencements uniquement sur les versions européennes de son moteur de recherche c'est-à-dire les ccTLDs des Etats européens (google.fr, google.it, etc.), mais pas sur google.com qui est pourtant accessible depuis le territoire européen. Mais une application de la décision de justice européenne sur google.com poserait en retour la question de l'extra-territorialité du droit européen. Les débats sur cette question sont, quant à eux, encore peu nombreux bien que soulevant des enjeux majeurs en termes de fragmentation juridique et des contenus de l'Internet

[156] Source : http://www.francetvinfo.fr/internet/google/deja-70-000-demandes-pour-le-formulaire-google-de-droit-a-l-oubli_638699.html
[157] Source : http://bourse.lesechos.fr/infos-conseils-boursiers/infos-conseils-valeurs/infos/google-organise-des-rencontres-en-europe-sur-le-droit-a-l-oubli-997561.php

1.4.2 Une certaine conception européenne de la gouvernance

En termes diplomatiques, l'UE peut également s'appuyer sur ses valeurs afin de porter la voix d'une gouvernance équitable et respectueuse de l'ensemble des parties prenantes. Certains Etats poussent de plus en plus à la mise en place d'un modèle intergouvernemental dans lequel les Etats seraient les acteurs principaux de la gouvernance sous l'égide de l'UIT. Si les Etats représentent certainement une force qui détient un rôle important dans la gouvernance, ils ne peuvent être les seuls acteurs ayant un droit de décision. Alors que les pays asiatiques et africains vont monter en puissance en nombre de populations en ligne, le rapport de force risque d'évoluer au profit d'Etats promouvant ce modèle. Aussi l'enjeu pour l'Europe est-il de garantir la conception d'un modèle multiparties prenantes en adéquation avec les valeurs de l'Europe tout en prenant acte du basculement dans le rapport de force.

Il est évident que l'on n'empêchera pas les Etats souhaitant pratiquer la censure de la mettre en place. On a observé dans la première partie que l'idée d'un Internet libre, ouvert et global n'était qu'un fantasme et échouait à faire face à la réalité des pratiques intentionnelles ou non. La fragmentation de l'Internet et du web est déjà une réalité. L'analyse fournie montre toutefois que le risque de voir émerger des Internets totalement souverains et nationaux est minime car l'interopérabilité des systèmes et des réseaux est la condition *sine qua non* à la réalisation des promesses économiques offertes par l'Internet, y compris dans les pays autoritaires. A ce titre en France, le Conseil National du Numérique soulignait dans son rapport du 7 mai 2013 pour Fleur Pellerin, Secrétaire d'Etat au Commerce extérieur, l'importance des valeurs de l'Union Européenne dans la stratégie numérique. En effet, la première recommandation du rapport précise que « *les valeurs de l'Union européenne sont des leviers essentiels à la construction d'une stratégie de négociation sur le volet numérique* ».

A ce titre, la stratégie « Compact for the Internet » évoquée en juin 2011 constitue un élément important de cet enjeu diplomatique. Elle évoque en effet une certaine conception de l'Internet et de sa gouvernance : « an Internet of **C**ivic responsibility, **O**ne Internet, that is **M**ulti-stakeholder, **P**ro-democracy, **A**rchitecturally sound, **C**onfidence inspiring, and **T**ranparenthly governed »[158]. L'Europe a des intérêts qu'elle ne fait pas valoir dans la situation actuelle à l'instar de nombreux autres Etats (hors Etats-Unis). Il en résulte des rivalités croissantes en fonction des intérêts de chacun. L'Europe ne pourra pas faire face à l'ensemble de ces rivalités tout en gardant en ligne de mire l'objectif de garder un Internet

[158] Source : http://europa.eu/rapid/press-release_SPEECH-11-479_en.htm?locale=en

global. Il faudra faire des concessions à l'échelle nationale sur les questions de censure notamment, en étant vigilant à l'échelle mondiale sur les évolutions en cours. D'autant plus que l'analyse montre très clairement l'intrication des enjeux économiques et politiques avec ceux de sécurité et de souveraineté.

L'Europe doit faire face à un double défi. D'un côté, le manque de confiance y compris au sein de l'UE qui incite les Etats-membres aux économies les plus avancées d'engager un repli national en matière de politiques numériques. De l'autre, la grande disparité des moyens des 28 pays de l'UE et la demande de coopération croissante des pays les moins avancés.

2 Les enjeux de souveraineté et de sécurité : l'Europe est-elle l'échelle pertinente ?

2.1 Fragmenter pour mieux contrôler ?

Les révélations d'E. Snowden sur les activités d'espionnage des systèmes d'information (SI) des alliés et partenaires stratégiques des États-Unis, dont la France fait partie, ont mis en lumière les enjeux de sécurité et de souveraineté liés à ces activités, de la part des États-Unis, mais aussi potentiellement (et sûrement) de la part d'autres acteurs étatiques, y compris entre alliés. Cette surveillance incite les États à renforcer les contrôles aux « frontières » du cyberespace, afin de prévenir et d'empêcher les intrusions qui peuvent porter atteinte à la souveraineté des Etats et à la sécurité des infrastructures vitales. D'emblée, il faut souligner que ces questions, comme tout le spectre du renseignement, relèvent de compétences strictement nationales. Si les coopérations interétatiques existent, principalement sur le plan bilatéral, elles sont régies par une stricte logique du « donnant-donnant », dans le cadre d'accords opaques.

La dynamique de fragmentation des réseaux et des systèmes d'information à des fins de sécurité et de souveraineté est susceptible d'entraîner des effets paradoxaux et non voulus. En effet, cloisonner les infrastructures vitales peut d'une part, se révéler difficilement réalisable d'un point de vue opérationnel et juridique : comment garantir l'application d'un droit national dans le cadre de plateformes mondiales utilisées pour les activités de l'État[159] ? Comment garantir l'application des mesures techniques et non techniques de sécurité au sein

[159] Les services de messagerie en ligne, ainsi que les moteurs de recherche, etc.

des infrastructures vitales[160], majoritairement opérées et détenues par le secteur privé ? D'autre part, la fragmentation posera des problèmes quant à la coopération internationale en matière de lutte contre la cybercriminalité ou de partage de l'information dans le domaine des alertes de cybersécurité notamment. Enfin, une fragmentation par cloisonnement pourrait aussi augmenter les risques d'escalade involontaire et de violence incontrôlée entre acteurs étatiques en l'absence de seuils de représailles clairement identifiés[161]. Aussi les bénéfices apparents de la fragmentation doivent-ils être évalués au regard des contraintes et des risques qu'ils engendrent ou pourraient engendrer pour la souveraineté et la sécurité des États. Par voie de conséquence, les dynamiques de repli souverain existantes ou latentes en Europe n'apparaissent pas comme étant la solution la mieux adaptée pour la préservation de la souveraineté et de la sécurité des États.

Inversement, certaines dimensions du cyberespace semblent nécessiter davantage de cloisonnement afin de renforcer la préservation de la souveraineté des Etats. C'est ce que laissent suggérer certaines des dynamiques actuelles, particulièrement pour la cyberdéfense militaire, un domaine éminemment régalien où la souveraineté nationale prévaut. Bien plus encore que pour la coopération interétatique en matière de défense classique, la coopération en matière de cyberdéfense est extrêmement délicate. Cela s'explique par l'interconnexion massive des réseaux et système d'information civils et militaires, également par le fait que les États sont encore réticents à partager leurs capacités défensives et offensives dans le cyberespace. La coopération pour la cyberdéfense se matérialise par l'échange d'informations relatives à la découverte de vulnérabilités par les organismes compétents (CERT, CIRC, SOC, etc.), dans la limite de la préservation de la sécurité et de la souveraineté nationale des États. En matière de cyberdéfense, les coopérations se feront ainsi plus facilement sur un plan bilatéral, dans une logique de choix réciproque[162]. Notons que la souveraineté nationale est un frein à la mise en place de capacités communes de cyberdéfense militaire, au sein de l'UE mais aussi à l'intérieur de l'OTAN, ce que nous allons démontrer.

Certaines dynamiques de fragmentation étaient perceptibles avant même les révélations d'E. Snowden, qui ont démontré de manière concrète quels étaient les enjeux de souveraineté et de sécurité liés à l'espionnage et à la surveillance des infrastructures vitales

[160] Les Opérateurs d'Importance Vitale (OIV) sont définis par l'article R1332-2 du Code de la défense français & par l'article R1332-1 du Code de la défense.
[161] Pour un examen complet des chaînes d'événements possibles, voir M. Libicki, *Crisis and Escalation in Cyberspace*, RAND Corp., 2012.
[162] J. Saiz, « La délicate collaboration internationale en matière de cyber-défense », Qualys Magazine http://magazine.qualys.fr/cyber-pouvoirs/collaboration-internationale-cyber-defense/

par des acteurs étatiques étrangers (alliés ou non). Prenant conscience de cette réalité, plusieurs responsables politiques nationaux, à la tête d'Etat européens ont accéléré les processus de fragmentation de certaines dimensions du cyberespace ; l'idée directrice est de préserver la souveraineté et d'améliorer la sécurité des infrastructures vitales nationales[163]. Or, dans le cyberespace, la fragmentation ne signifie pas forcément un meilleur contrôle ni une meilleure maîtrise des « frontières » dudit espace. Elle est techniquement complexe à mettre en place, économiquement et politiquement délicate à maintenir. Néanmoins, la souveraineté étant un impératif – un Etat-nation est un Etat souverain -, particulièrement dans le domaine de la défense et du renseignement et plus encore dans celui de la cyberdéfense, il faut évaluer la pertinence de l'échelle européenne (UE) comme cadre de détermination, de mutualisation des efforts et de mise en place de solutions communes aux Etats membres de l'UE.

2.2 L'incapacité fonctionnelle des forums interétatiques européens à enrayer les dynamiques de fragmentation

Les deux organisations les plus à même de fournir un cadre normatif et institutionnel pour trouver des solutions communes aux enjeux de souveraineté et de sécurité liés à la cybersécurité et à la cyberdéfense en Europe sont l'Union Européenne (UE) et l'Organisation du Traité de l'Atlantique Nord (OTAN).

Au sein de l'UE, les questions de cybersécurité et de cyberdéfense ont été abordées depuis la fin des années 1990 par le prisme de la sécurisation des moyens d'information et communication. L'enjeu est de protéger les libertés individuelles des citoyens européens, et de garantir la poursuite et la pérennité de leurs activités commerciales et économiques (biens et de services) au sein des frontières de l'UE[164]. Par la suite, la recherche systématique de la sécurisation des TIC s'est élargie à l'ensemble des fonctionnalités couvertes par leur utilisation, ouvrant ainsi la voie à la sécurité des infrastructures de communication et d'accès à l'information (Internet, réseaux de téléphonie mobile, etc.).

[163] C'est notamment le cas de la France et de l'Allemagne ; voir http://www.ssi.gouv.fr/fr/menu/actualites/nouvelle-france-industrielle-la-feuille-de-route-cybersecurite-validee.html , et http://junge-transatlantiker.de/wp-content/uploads/2014/08/Memorandum-NSA-2.pdf

[164] Parmi ces mesures, on peut citer cette liste non-exhaustive : Directive 1999/93/EC, Directive 2000/31/EC, , Directive 2002/19/EC, Directive 2002/20/EC, Directive 2002/21/EC, Directive 2002/22/EC, Directive 2002/58/EC, Commission Decision 2002/627/EC.

Cependant, les actions de l'UE souffrent d'une double limite. La première est d'ordre politique ; elle se manifeste par la volonté des Etats de limiter le mandat d'action de l'UE en matière de cybersécurité. Cette volonté politique, ardemment défendue par les pays les plus avancés en matière de capacités cyber et TIC (l'Allemagne, la France, le Royaume-Uni), découle directement des enjeux de souveraineté exposés à toute tentative de régulation excessive de la part de l'UE, i.e. de la Commission européenne, au détriment des régulations nationales. L'exemple le plus flagrant et le plus concret de cette limitation imposée par les Etats membres est celui de l'ENISA, dont le mandat est d'une ampleur réduite. Cette agence européenne en charge de la cybersécurité n'a qu'un rôle de conseiller et d'expertise ; elle ne dispose pas du pouvoir d'imposer des mesures contraignantes aux Etats membres de l'UE ni de capacité opérationnelle qui lui donnerait plus de pertinence.

La seconde limitation est d'ordre fonctionnel et découle de la première. L'UE ne dispose ni du mandat, ni des moyens nécessaires pour devenir l'acteur référent en matière d'actions de cybersécurité en Europe. D'une part, au niveau du mandat, le principe de subsidiarité inscrit dans le traité de Lisbonne[165] est fondamental pour le fonctionnement de l'Union Européenne : il permet de déterminer le niveau d'intervention le plus pertinent dans les domaines de compétences partagées entre l'UE et les États membres. Or, en matière de cybersécurité et de cyberdéfense, le niveau national s'impose, de par la volonté de faire prévaloir la souveraineté de chaque Etat membre. D'autre part, au niveau des moyens, si l'UE dispose d'outils juridiques contraignants pour imposer des normes, elle ne dispose pas des capacités opérationnelles qui lui permettraient d'agir au-delà de ses propres systèmes d'information. L'ENISA n'a ainsi qu'une fonction de conseiller technique, malgré le renforcement de son mandat en mai 2013[166], ce qui a accru son rôle dans l'élaboration de politiques et de législations européennes relatives à la cybersécurité. Les travaux de R&D que l'on y mène visent à améliorer les standards de sécurité des TIC. Il reste que l'ENISA est l'acteur de référence sur ces questions, pour ce qui touche à la coopération entre l'UE et d'autres acteurs internationaux.

La dynamique de fragmentation du cyberespace en Europe est la plus marquée lorsque les questions de cyberdéfense sont en jeu. Les capacités militaires de cyberdéfense d'un État, centrées sur les moyens de détection et de réaction face aux cyberattaques, ne sauraient être

[165] http://europa.eu/legislation_summaries/institutional_affairs/treaties/lisbon_treaty/ai0017_fr.htm
[166] Regulation (EU) No 526/2013

mises en commun au niveau UE. La Stratégie de Cybersécurité de l'Union Européenne[167], si elle mentionne le besoin d'améliorer les capacités de cyberdéfense pour les missions militaires de l'UE, prend la précaution d'annoncer qu'une « évaluation préalable des besoins identifiés » sera effectuée avant toute décision commune. Le groupe de travail qui est chargé de cette évaluation se heurte aujourd'hui à une faible volonté de coopération de la part des États membres, ce qui s'explique par une anticipation négative quant à l'aboutissement de ce projet, principalement à cause de son manque de pertinence. Ce manque de pertinence, particulièrement mis en avant par les États qui disposent des capacités pour être les « nation-cadres » des missions militaires de l'UE, repose sur des arguments technico-militaires : la redondance avec les outils existants ou développés dans le cadre de l'OTAN ; l'application du principe de subsidiarité ; les enjeux de souveraineté. Selon ces arguments, la décision de créer et mettre en place une capacité permanente de cyberdéfense militaire pour l'UE ne serait pas fondée et justifiée[168]. Comme l'exprime un officier de l'État-Major des Armées françaises, l'organisation au niveau européen d'une intervention en cas de cyberattaque majeure transfrontalière est, dans l'état actuel des capacités opérationnelles militaires européennes, problématique : « *Dans une telle situation la France ne veut pas d'autorité supranationale qui nous imposerait des mesures. Une intervention au niveau européen serait donc compliquée*[169] ». Cette déclaration nous renvoie aux obstacles dressés devant le projet de mise sur pied d'une « Europe de la Défense ». Dès lors, il semble que l'Union Européenne ne soit pas le cadre institutionnel qui permettrait de briser les dynamiques de fragmentation du cyberespace en Europe, tant les enjeux de souveraineté et de sécurité freinent les États membres dans la création de capacités communes. En l'état des choses, l'UE doit se limiter à un rôle de « facilitateur » de coopération pour les États membres, en proposant des structures qui agissent comme « point de contact » en cas de besoin exprimé *ad hoc*. Il en est ainsi parce que les Etats membres de l'UE, y compris les plus allants au plan européen, ne veulent pas aller au-delà de ce qui existe.

Au sein de l'OTAN, les choses ont beaucoup évolué. La prise de conscience des enjeux politico-militaires liés au cyberespace et de l'impact potentiel de cyberattaques de grande envergure contre les systèmes d'information implantés dans les appareils de défense

[167] Cybersecurity Strategy of the European Union : An Open, Safe, and Secure Cyberspace, février 2013
[168] Entretiens avec les personnes en charge des appels d'offres CAP.10.111.2012 & 12.CAP.OP.332 pour l'Agence Européenne de Défense, pilote des projets pour l'Union Européenne.
[169] Entretien J.Saiz avec un officier de l'État Major chargé des questions cyber, Qualys Magazine, *op. cit.*

des États (technologies de communication nécessaires aux prises de décisions, systèmes d'armement) date de l'année 2007. Depuis les attaques de Tallinn, l'OTAN a successivement adopté des mesures permettant d'inclure les missions de cyberdéfense dans son mandat, bien que celles-ci soient restées longtemps limitées à la protection des infrastructures de l'Organisation[170].

Ainsi, le Conseil de l'Atlantique Nord adopte en janvier 2008 la première Politique de Cyber Défense (Cyber Defense Policy), faisant prendre une dimension politique et stratégique de première importance aux enjeux de cyberdéfense au sein de l'OTAN. Le Sommet de Bucarest (avril 2008) entérine la création de deux nouveaux organismes : l'Autorité de Coordination de la Cyber Défense (Cyber Defense Management Authority), chargée de coordonner les réponses des alliés à de potentielles cyberattaques, et le Centre d'Excellence de Cyber Défense de l'OTAN (Cooperative Cyber Defence Centre of Excellence), constitué en Estonie en mai 2008 afin de conduire et dynamiser la recherche autour des dimensions stratégiques et légales de la question. En 2012, lors du sommet de Lisbonne, le Conseil annonce la révision de la Politique de Cyberdéfense de l'Alliance. Après d'âpres tractations et négociations politiques, le texte adopté six mois plus tard ne fait que rappeler le mandat de l'OTAN en matière de cyberdéfense : celle-ci défendra ses réseaux et systèmes d'information, les États membres défendant les leurs. Ainsi, malgré l'institutionnalisation des actions de l'Alliance en matière de cyberdéfense, l'OTAN semblait elle aussi se heurter aux enjeux de souveraineté et de sécurité mis en avant par les États membres. Pourtant, la question progresse dans les instances de l'OTAN et, fin 2013, un Centre de réaction aux attaques a été mis sur pied[171]. Il peut fournir des équipes volantes aux pays qui font la demande d'une assistance. Pour les pays non membres de l'OTAN, cette demande doit être acceptée au niveau du Conseil de l'Atlantique Nord. En juin 2014, les ministres de la Défense des pays de l'OTAN ont décidé de mettre à jour la Politique de Cyberdéfense de l'Alliance. Reconnaissant l'omniprésence du cyberespace dans l'environnement international conflictuel contemporain, les ministres ont décidé de reconnaître explicitement que la clause de défense commune telle qu'énoncée dans l'article 5 du Traité de l'Alliance pouvait s'appliquer au cyberespace, en cas d'attaque majeure. Bien que l'appréciation de cette application soit encore établie *ad hoc*, l'adoption du principe est une avancée politique notable. De plus, les ministres se sont mis d'accord sur le renforcement de la collaboration entre États membres, notamment en matière

[170] 2008 Cyber Defense Policy,
[171] Les Rapid Reaction Team étaient déjà évoquées dans la doctrine de 2008, mais leur mise en œuvre date de 2013.

d'échange d'information et d'assistance mutuelle, de multiplication d'exercices de simulation, ou encore d'accroissement de la coopération avec le secteur industriel. Les mesures ont été officiellement entérinées lors du sommet de Newport (Pays de Galles), les 4-5 septembre 2014, ce qui témoigne d'une volonté politique commune de renforcer la politique existante[172]. La crise ukrainienne, le rattachement manu militari de la Crimée et l'intégration d'une composante « cyber offensive » dans la stratégie militaire russe auront peut-être accéléré un processus entamé en amont.

Néanmoins, étant donnée la place primordiale qu'occupent les États-Unis au sein de cette Alliance, plusieurs dimensions doivent être considérées dans la lecture du positionnement des États européens en matière de coopération pour la cyberdéfense au sein de l'OTAN. Nous avons évoqué plus haut le problème de redondance de procédures et d'outils que créerait la mise en place d'une capacité militaire UE de cyberdéfense. L'idée sous-jacente, ardemment défendue par Washington, est de ne pas s'encombrer de normes et standards de sécurité supplémentaires « spécifiques UE » quand ceux développés pour l'OTAN sont déjà existants et ont fait leurs preuves. Développer et imposer de nouveaux protocoles constitueraient une charge financière supplémentaire inutile, et une contrainte logistique et opérationnelle qui entraverait l'interopérabilité entre les Alliés. C'est dans cet esprit, pour éviter les « duplications inutiles » que les accords de Berlin Plus avaient été négociés[173] ; la même approche pourrait être appliquée aux capacités de cyberdéfense. Cet argument constitue pour Washington un atout considérable pour contrarier toute velléité européenne en matière de cyberdéfense, qui aurait pour objectif le renforcement de l'UE, et permet également de promouvoir l'industrie américaine de cybersécurité en Europe, notamment auprès des pays les moins développés dans le domaine. Pourtant l'OTAN a vocation à rester l'institution privilégiée des États européens en matière de défense et dans la détermination des standards nécessaires à l'interopérabilité de forces militaires en action, y compris dans le cadre de « coalitions de bonnes volontés », avec ce que cela implique dans le domaine de la cyberdéfense. Les révélations d'E. Snowden n'ont pas ébranlé le cadre atlantique, référence de la plupart des Etats européens pour la défense collective (les missions civilo-militaires de l'UE sont pensées dans une logique de complémentarité).

[172] NATO, Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014, § 72-73.
[173] Conseil de l'Union européenne, EU-NATO: The Framework For Permanent Relations And Berlin Plus, http://www.consilium.europa.eu/uedocs/cmsUpload/03-11-11%20Berlin%20Plus%20press%20note%20BL.pdf

Ainsi, les enjeux de souveraineté et de sécurité des États européens dans le cyberespace sont à l'origine de plusieurs dynamiques antagonistes : d'une part, la prise de conscience, par les révélations d'E. Snowden, de l'urgence de rétablir et de préserver la souveraineté stratégique des États par un renforcement des mesures de sécurité, mais d'autre part, la compréhension du besoin de continuité dans les activités de sécurité et de défense internationale, qui se traduit par le nécessaire maintien d'une interopérabilité entre forces armées et par le nécessaire besoin d'échange et de partage d'informations cyber et non cyber.

Dans les faits, l'UE ne semble pas constituer le cadre idéal pour développer une capacité militaire commune de cyberdéfense : son mandat sur le plan de la cybersécurité reste limité par le principe de subsidiarité, ledit principe renvoyant aux enjeux de souveraineté et de sécurité nationale des Etats membres. Le périmètre d'action des agences européennes reste donc très limité et ce de par la volonté des gouvernements. Il faut conserver à l'esprit que l'UE, en dernière analyse, est une Europe intergouvernementale.

Le champ d'action de l'OTAN, lui aussi, reste encore limité : d'une part, les désaccords politiques limitent le mandat de l'Alliance à la protection de ses réseaux et systèmes d'informations, d'autre part, la mise en commun de capacités défensives/offensives militaires pouvant être déployées par par l'Alliance en cas de crise, se heurte à des limites tant techniques que politiques. Les États membres les plus avancés dans le domaine n'accepteront *a fortiori* pas d'effectuer un transfert de technologies qui risquerait d'affecter leur sécurité. L'Alliance, comme l'UE, ne joue encore qu'un rôle de conseiller en offrant son expertise et ses outils de manière *ad hoc* aux États qui en exprimeraient le besoin. Il faut pourtant insister sur les avancées successives opérées dans cette structure de défense collective. Le durcissement du contexte international et la traduction en termes concrets du thème de la « cyberguerre » pourraient mener les Etats membres de l'OTAN à aller plus loin qu'ils ne le voulaient initialement, nécessité faisant loi.

Pourtant, il appert que le cadre national, pour les Etats les plus en pointe, reste premier. Dans le domaine de la coopération interétatique, les discussions sont avant tout bilatérales et c'est dans ces forums privilégiés que les choses se font et se négocient. C'est précisément la position que privilégie la France actuellement : « *plutôt qu'un dispositif centralisé qui devrait tout faire, nous privilégions l'entraide internationale, au cas par cas et selon des relations de confiance existantes*[174] ». A certains égards, il semble que l'étroite relation anglo-américaine qui existe en matière de renseignement, de partage de l'information

[174] Entretien J.Saiz avec un officier de l'État Major chargé des questions cyber, Qualys Magazine, *op. cit.*

et de cyberdéfense fasse figure de modèle pour les alliés les plus importants des Etats-Unis : la France comme l'Allemagne cherchent à renforcer leur « *special relationship* » propre avec Washington (limitation de l'espionnage réciproque et plus grand partage du renseignement). Mises en évidence par les révélations d'E. Snowden, ces attentes ainsi que les coopérations bilatérales existantes expliquent peut-être la réserve et la relative discrétion de bien des gouvernements européens dans cette affaire.

Cependant, le primat de la souveraineté et la coopération bilatérale qui s'ensuit, tendent à accentuer les dynamiques de fragmentation du cyberespace, en favorisant le recours à des dialogues « privés » au détriment de solutions multipartites. La cyberdéfense militaire, ainsi que les capacités cyber de renseignement, semblent aujourd'hui constituer des enjeux trop sensibles et trop importants, liés à la souveraineté des États, pour sortir du cadre national. Toutefois, les États ne ferment pas complètement la porte à l'amélioration substantive du rôle des institutions internationales et régionales qui pourraient constituer, pour les États européens, un cadre utile pour contrebalancer l'influence américaine au sein de l'OTAN et prévenir celle d'adversaires potentiels, à l'extérieur des instances euro-atlantiques. Comme le précise un officier français de l'EMA en charge des questions cyber : « *Nous préférerions que l'Union Européenne se saisisse vigoureusement de ces sujets car entre les Etats-Unis et la Chine, il ne reste que l'espace européen. Mais les 28 n'ont pas encore pris position fermement, notamment sur la base industrielle et technologique qui fonde cette souveraineté cyber*[175] ». On notera cependant le jeu habituel qui consiste à invoquer de manière rituelle l'UE, tout en limitant la montée en puissance de ce cadre, au nom de la souveraineté nationale, pour ensuite déplorer l'insuffisante affirmation de l'UE, voire la mettre en accusation. L'UE n'est pas un acteur global qui s'autosaisirait : les décisions essentielles sont prises par ses Etats membres, à l'unanimité. Sur le plan de la cyberdéfense comme sur celui de la défense, les Etats européens privilégient le cadre national et le cadre atlantique, y compris les Etats les plus engagés dans la « construction européenne ». Cette réalité de base n'est guère favorable à la promotion du cadre européen en matière de cyberdéfense. Au vrai, les efforts en matière de cyberdéfense sont menés dans un cadre national-étatique, ce qui permet ensuite de compter dans les négociations bilatérales.

Les enjeux de souveraineté et de sécurité au sein de l'UE constituent un frein certain à la coopération notamment en matière de défense et de sécurité mais pas seulement. La dynamique du manque de confiance dans laquelle ils s'inscrivent, nuit également au

[175] *Ibid.*

développement de coopération industrielle et économique sur le plan numérique, incitant les Etats européens les moins avancés à se tourner vers l'OTAN et les Américains dans le but d'acquérir les outils pour le développement et la protection de leurs réseaux.

Afin d'illustrer les différents enjeux mis en lumière tout au long de cette partie, nous consacrerons un focus sur un cas d'étude, celui du « *cloud* souverain » qui est particulièrement symptomatique des enjeux auxquels l'Europe doit faire face que ce soit en matière de politiques industrielles, d'enjeux de souveraineté, de la question des données ou encore des enjeux juridiques notamment en matière d'extra-territorialité. En effet, le *cloud computing* crée une double nervosité pour l'Europe. D'abord, on observe la concentration des données dans les mains de quelques acteurs, les géants du web américains (Amazon, Microsoft, Google) dont on a vu leurs puissances mais aussi leurs liens avec les agences de renseignement américaine. Mais le développement des offres de *cloud* en Europe interroge également les pratiques numériques des entreprises et des Etats alors qu'ils abandonnent complètement la gestion de leurs données à une plateforme tiers.

3 Le cas d'étude du « *cloud* souverain »

Le « *cloud computing* » constitue l'une des tendances les plus significatives de l'évolution récente en matière de gestion des systèmes automatisés de traitement de l'information. Il traduit, en effet, la montée générale d'un processus d'intégration de ces systèmes au sein du cyber espace. On peut situer dans les années 1990-2000 l'émergence et le développement d'un processus de mise en réseau qui a permis, grâce à l'extension des différents réseaux, réseaux locaux ou réseau Internet, de faire communiquer entre eux des matériels informatiques de différente nature (micro-ordinateurs, imprimantes, serveurs, terminaux divers…), indépendamment de leurs caractéristiques propres (fabricants, systèmes d'exploitation…) Ce processus de mise en réseau a ainsi permis d'aller au-delà de la phase de décentralisation qui avait vu se disséminer les matériels informatiques chez les usagers, dans un premier temps, sous la forme de terminaux asservis à un système central puis, dans les années 1980, sous celle de micro-ordinateurs capables de fonctionner de manière autonome. Le développement du « *cloud computing* » s'analyse non pas comme un retour à une informatique centralisée (qui était celle des années 1960) puisqu'elle s'appuie précisément sur la constitution d'un réseau fondé sur l'interconnexion systématique d'appareils distants, mais plutôt comme une forme d'intégration poussée qui accentue le lien de dépendance des matériels distants vis-à-vis d'un système central dont le rôle est considérablement renforcé et

dont la très grande puissance procure un surcroît d'efficacité dans le traitement, le stockage et la diffusion des données .

Selon le National institute of Standards and Technology, le « *cloud computing* » se définit comme suit : « *cloud computing* is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. »[176]

Cette manière nouvelle de concevoir et de gérer les systèmes informatiques se caractérise par cinq traits fondamentaux :

- Un service sur mesure : l'utilisateur (ou celui qui met à sa disposition un terminal) peut configurer le matériel à la mesure exacte de ses besoins ou des nécessités de sa mission. Il est possible d'ajuster individuellement les temps d'accès au service central, le volume de stockage, le type de logiciels disponibles, les données accessibles ou non…
- Une très grande simplicité d'accès : les utilisateurs peuvent disposer de leurs ressources informatiques dès lors qu'ils sont connectés au système central, peu importe le lieu où ils se trouvent ou le type de terminal qu'ils utilisent.
- Un partage des ressources : les ressources disponibles au niveau central (capacités de stockage, de traitement, etc.) sont partagées entre de multiples utilisateurs. Un processus d'optimisation est mis en place par le gestionnaire du système pour faire en sorte de réduire le coût d'accès, de stockage et d'utilisation par le meilleur emploi possible de ces ressources. Pour l'utilisateur, ce processus d'optimisation est transparent sauf pour lui à fixer des contraintes spécifiques, par exemple le lieu de stockage des données qu'il introduit dans le système.
- L'élasticité des ressources : le prestataire du service doit être en mesure de faire face à toute variation quantitative ou qualitative de la demande. Ses capacités de traitement de l'information doivent pouvoir s'adapter rapidement au besoin de l'utilisateur, qu'il s'agisse par exemple d'une augmentation de l'espace de stockage requis ou de l'accès à une ressource logicielle dont il n'avait jusque là pas l'utilité.

[176] P Mell et T Grance, 2011, The NIST Definition of Cloud Computing, NIST Special Publication, n° 800-145, US Department of Commerce, Computer Security Division, Septembre

- La quantification de l'usage : le partage des ressources entre différents utilisateurs repose sur le principe utilisateur / payeur, ce qui entraîne le besoin de quantifier et de facturer l'usage que chacun fait des ressources mises à disposition. La logique de propriété de la ressource informatique intégrée dans un micro-ordinateur (mise à niveau des composants ou achat de barrettes mémoire supplémentaires en tant que de besoin, acquisition de licences pour les différents logiciels…) laisse la place à une logique d'usage plus proche de la location d'une ressource en fonction d'un besoin qui est susceptible de varier dans le temps.

On notera pour terminer que le principe et les caractéristiques du « *cloud computing* » peuvent s'appliquer à un objet plus ou moins large selon la volonté de l'utilisateur : de la fourniture d'une infrastructure physique de stockage à l'ensemble des ressources physiques et logicielles nécessaires à la réalisation d'un traitement informatisé. De l'organisation traditionnelle dans laquelle l'utilisateur gérait l'ensemble de son infrastructure, de ses logiciels et de ses données jusqu'à la solution « Software As A Service » où l'ensemble est confié à un prestataire extérieur, le « *cloud computing* » offre une variété de solutions qui concerne aussi bien les entreprises que les administrations civiles ou militaires.

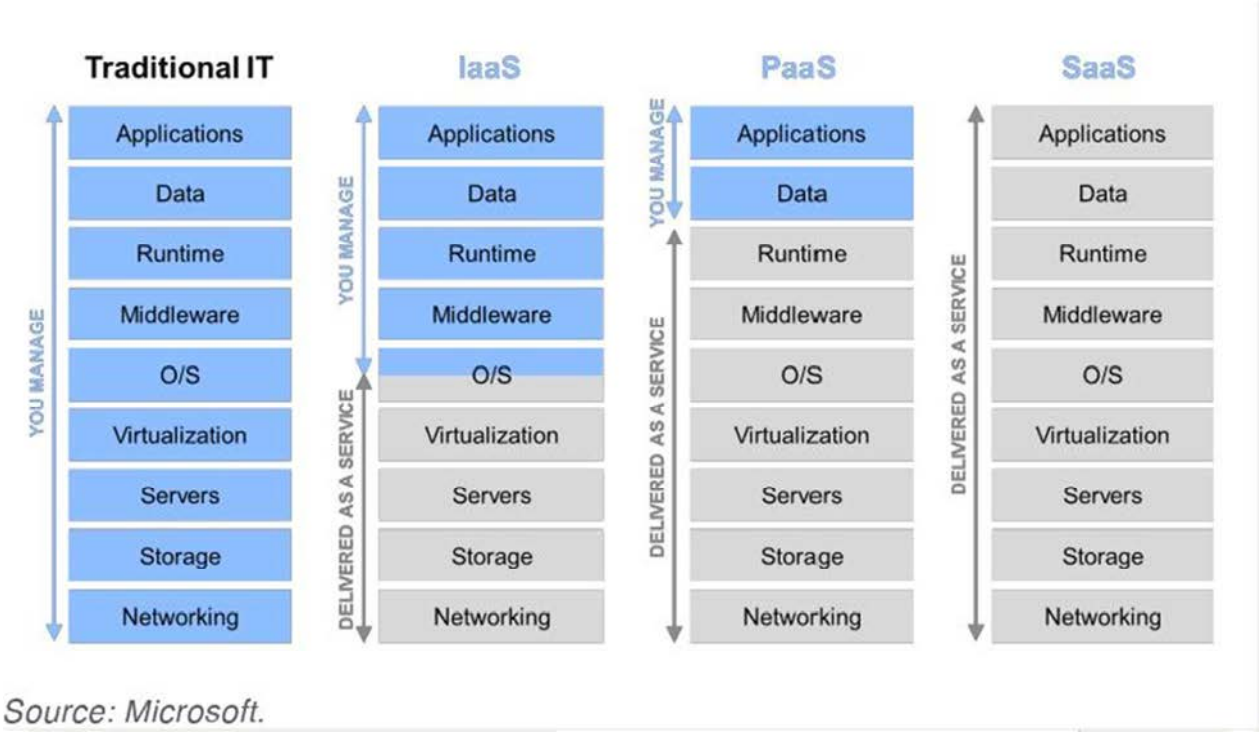
3.1 Les enjeux de sécurité du Cloud : critères d'évaluation des risques

Le développement rapide du « *cloud computing* » à destination des entreprises et des administrations pourrait annoncer une révolution en termes de sécurité informatique. En effet, la sous-traitance du stockage des données, ainsi que des machines et des logiciels intervenant dans le traitement des données, semble repousser la question de la sécurité de l'usager au prestataire de service.

Le prestataire est en théorie responsable de la sécurisation des services qu'il offre, de la maintenance et de la mise à jour du matériel engagé. L'usager, s'il est toujours responsable de sa plateforme physique pour accéder au « *cloud* » (PC, tablette, téléphone ou autres), se verrait donc en grande partie dégagé des préoccupations afférentes à la gestion du parc informatique utilisé et à la protection des données stockées. Ce transfert de responsabilité à un

prestataire de service spécialisé pourrait permettre l'émergence de sites beaucoup mieux sécurisés, réduisant d'autant les menaces en termes de cyberattaques et de cybercriminalité.

Fig. 9 – Schéma de sous-traitance



Source: Microsoft.

Néanmoins, ces remarques liminaires ne sont malheureusement que théoriques, car en termes de sécurité, l'essentiel des responsabilités reste défini par le contrat entre le prestataire et l'usager, contrat qui, du fait de la structure du marché et du monopole de quelques géants (Google, Amazon Web Services, IBM, Microsoft), est souvent rédigé en faveur du prestataire. Il est de notoriété publique que les contrats d'adhésion, dont le contrat qui unit l'utilisateur et le prestataire en matière de *cloud computing* sont presque systématiquement déséquilibrés et les premiers retours d'expérience sur les difficultés contractuelles rencontrées par les utilisateurs (disponibilité réelle du service, portabilité des données…) confirment largement la règle.

De fait, la diffusion du « *cloud computing* » crée aujourd'hui de nouveaux enjeux de sécurité pour les usagers. Citons ici les trois principaux, à savoir : la disponibilité des données, leur intégrité et leur confidentialité. La disponibilité des données à tout moment suppose à la fois une logistique irréprochable de la part du prestataire (en terme de matériel, de logiciels, de maintenance) et une localisation des infrastructures physiques permettant une

excellente connexion aux autoroutes de l'information, à proximité des points de raccordement aux « *backbones* » de l'Internet. Cette question de la disponibilité suppose donc de pouvoir gérer des problèmes de débit de transfert, de fiabilité du transfert, mais aussi des questions très pragmatiques de gestion des infrastructures, comme la question de l'approvisionnement énergétique (les *data centers* impliquent un approvisionnement conséquent et permanent, une coupure d'électricité pouvant générer l'indisponibilité des données et des services pour un nombre important de clients) ou celle de la sécurisation des sites (leur implantation étant souvent visible, dans les zones industrielles périurbaines, ou à proximité de grand nœuds de communication – leur sécurisation suppose donc des moyens en termes humains et technologiques).

L'intégrité des données est un enjeu primordial, car la corruption ou la perte de données peut s'avérer dramatique suivant le secteur d'activité concerné (administration publique, secteur bancaire, secteur de la santé, etc.). Par ailleurs, la perte d'expertise technique de l'usager concernant le traitement et le stockage des données le rend particulièrement dépendant du prestataire dans ces domaines. Or, cet aspect de la perte d'intégrité des données est souvent au cœur de la relation contractuelle liant le client au fournisseur. Les clauses de non-responsabilité peuvent le cas échéant dédouaner le prestataire en cas de dommages, de pertes ou de litiges. D'où la nécessité d'un cadre juridique protecteur et d'une relation équitable entre le prestataire et le client. Toutefois, des solutions techniques existent pour rendre plus hypothétiques la perte de données, et les gros fournisseurs proposent des offres plus ou moins sécurisées suivant la demande. Une solution couramment utilisée est la duplication des données sur deux sites différents, permettant notamment de prévenir le risque d'une destruction matérielle (catastrophe naturelle, attaques criminelles, etc.). Cette solution pose néanmoins le problème de la localisation des données et de leur confidentialité. En effet, la localisation physique des données pour le client est souvent difficile (sauf clauses contractuelles spécifiques), d'autant que celles-ci peuvent être hébergées sur plusieurs sites différents. Cette localisation est encore plus hypothétique dans le cas d'une redondance et d'une duplication. Or la localisation peut influer sur la confidentialité des données, comme le montre l'exemple des autorités américaines, qui pour des raisons de sécurité nationale, en vertu du *Patriot Act*, peuvent exiger d'accéder aux données stockées sur leur territoire (ou hébergées par une entreprise de droit américain – voir plus loin chapitre III).

La confidentialité des données est donc une préoccupation croissante auprès des usagers du « *cloud computing* », ceci dans un contexte de méfiance généralisée vis-à-vis des

fournisseurs américains, suite à l'affaire Snowden. Cette protection est par nature délicate du fait même de la technologie du « *cloud* », qui induit l'usage d'infrastructures mutualisées, et qui reste potentiellement accessible aux régulateurs locaux, voire à des régulateurs qui entendent faire prévaloir une application extra territoriale de leurs propres règles locales. Le risque de fuite est accentué par le manque de transparence concernant la localisation des données, et donc le manque de visibilité concernant la réglementation applicable, ou encore par le nombre d'acteurs intervenant à chaque niveau du « *cloud* ». Aussi, la bonne pratique suppose-t-elle de la part du client un chiffrement systématique des données considérées comme sensibles (voire la non utilisation du « *cloud* » pour des données stratégiques ou vitales). Les solutions de chiffrement permettent en théorie de ne rendre les données accessibles qu'aux interlocuteurs identifiés et autorisés à accéder aux informations par l'entremise d'une clef de déchiffrement. Les principales firmes du *cloud* proposent d'ailleurs à leur client leur propre solution de chiffrement (comme le *S3 client-side encryption* d'Amazon Web Services). Par ailleurs, elles développent également des réponses juridiques face aux réglementations intrusives des pouvoirs publiques. Ainsi, IBM France rassurait ses clients nationaux en 2012 en affirmant qu'IBM France étant une entreprise de droit français, il n'y aurait donc aucune raison de s'inquiéter quant à la portée du *Patriot Act* sur les clients français désirant héberger leurs données sur le territoire national. Ce faisant, ils reconnaissaient néanmoins l'importance de la localisation des données, ne serait-ce qu'en termes de législation et de souveraineté nationale.

3.2 *Cloud computing*, maîtrise des processus informationnels, souveraineté nationale.

En quoi, le *cloud computing* qui est, en première lecture, une réponse technique et managériale relevant de la responsabilité individuelle de chaque administration ou entreprise (ou tout autre acteur) en matière d'organisation de ses systèmes de traitement d'information induit-il des questionnements relatifs à la souveraineté étatique et à un éventuel risque de « balkanisation du web » ?

L'essentiel de l'offre de services se concentre entre un petit nombre d'entreprises qui ont conçu et développé le principe et les modalités du *cloud computing* et qui captent une grande partie d'une demande en très forte croissance : Amazon Web Services, Microsoft, IBM, Google. Le fait que la plus grande part du *cloud computing* soit ainsi sous le contrôle

d’opérateurs américains entraîne une domination des principes et des normes américaines en matière de régulation des activités.

D’une part, les opérateurs américains proposent à leurs clients de définir le cadre de leurs relations à venir à travers des dispositifs contractuels issus de l’esprit et des techniques en vigueur aux Etats-Unis, notamment de la « *soft law* » qui se distingue sensiblement sur le fond et sur la forme des règles en vigueur dans les pays de Droit continental comme la France. C’est ainsi que les principes de protection des données privées ou les règles relatives à la vie privée donnent naissance à des dispositions matérielles plus protectrices en Europe (en France en particulier) qu’aux Etats-Unis. L’entrée dans le *cloud computing* s’accompagne donc d’une insertion volontaire des acteurs économiques publics et privés dans un tissu de relations contractuelles qui font prévaloir une philosophie et des règles majoritairement issues du Droit américain. On ne saurait reprocher à ceux qui ont inventé les concepts et les techniques du *cloud computing* de s’appuyer sur le cadre juridique qui est le leur. Il serait également tout aussi fallacieux de ne voir que des inconvénients et des dangers dans l'application du Droit américain. Mais, on ne saurait pas davantage constater l’emprise progressive d’un Droit étranger sur un domaine essentiel du fonctionnement et de la compétitivité de l’ensemble des acteurs économiques français et européens sans se poser la question des avantages et des limites, des vulnérabilités ou des contraintes qui sont ainsi créés et des éventuels moyens d’y remédier.

D’autre part et surtout, au-delà de l’emprise du Droit américain que les mécanismes contractuels tendent à favoriser du fait de la multiplication à l’infini des décisions prises individuellement par chacun des acteurs qui recourent au *cloud computing*, les autorités politiques et judiciaires des Etats-Unis déploient une politique délibérée de régulation extraterritoriale qui les amènent à vouloir faire appliquer les règles propres du Droit américain à des situations où elles empiètent directement et massivement sur la compétence d’autres autorités souveraines. A deux reprises en 2014, les juges américains ont ainsi ordonné à Microsoft de fournir des données appartenant à un client étranger et stockées dans un *data center* situé en Irlande, considérant que le critère d’application de la loi américaine n’était pas le lieu de stockage des données mais la nationalité du prestataire de service à qui elles étaient confiées. En l’occurrence, Microsoft étant une firme américaine, elle est soumise à l’obligation de fournir les données requises par l’administration et ne peut s’y soustraire du seul fait que les données appartiendraient à des clients étrangers et seraient stockées en dehors des Etats-Unis. La solution n’est pas pour surprendre dans la mesure où les gouvernements

américains successifs cherchent à donner le plus large rayon d'action possible aux normes qu'ils jugent essentielles dans la lutte contre le crime ou la fraude, *a fortiori* contre le terrorisme ou l'espionnage. On se souvient que la loi Sarbanes Oxley (SOX), prise à la suite des faillites spectaculaires du début des années 2000, s'était traduite par l'instauration de mécanismes de « *whistleblowing* » qui imposaient aux sociétés cotées aux Etats-Unis de mettre en place des dispositifs de dénonciation anonyme des comportements frauduleux ou contraires à l'éthique des entreprises, les données ainsi recueillies devant permettre de sanctionner les coupables et de minimiser les conséquences fâcheuses de dérives des dirigeants ou de leurs employés. La justice américaine avait déjà considéré que ces dispositions devaient s'appliquer à toute société cotée aux Etats-Unis, qu'elle soit américaine ou non, et devaient être mises en œuvre dans tous leurs établissements et filiales aux Etats-Unis ou dans le monde. Il en découlait, par exemple qu'une entreprise française cotée aux Etats-Unis devait se soumettre à la loi SOX et mettre en place les dispositifs de dénonciation partout dans le monde, y compris en France où ils étaient directement contraires à des principes fondamentaux du droit du travail ou des libertés publiques. Dans le cas récent de l'entreprise Microsoft, on voit que les précautions visant à instaurer un rapport de confiance entre le prestataire et ses clients, précautions évoquées précédemment, se trouvent prise à revers par une politique publique qui témoigne d'une volonté de contrôle étendu.

Il découle de ce double processus, de domination des normes contractuelles d'origine américaine et de politique volontariste en faveur d'une application extraterritoriale du droit américain par les autorités publiques, une menace directe pour la souveraineté des autres Etats dont les systèmes normatifs sont ainsi contestés dans leur substance matérielle aussi bien que dans leur espace normal d'application. Cette intrusion d'une loi étrangère dans l'espace de souveraineté des autres Etats et la perspective pour les acteurs privés de devoir se soumettre aux règles du Droit américain sont manifestement de nature à susciter des réactions régionales ou nationales consistant non seulement à réduire le marché des firmes américaines aujourd'hui dominantes mais également à mettre en place des barrières (obligations d'implantation des *data centers*, configuration des réseaux et des circuits d'information, normes de transfert des données sensibles…) constituant autant de sources de fragmentation du cyberespace et de constitution d'îlots soumis à des réglementations spécifiques.

3.3 Régionalisation du Cloud : vers plus de souveraineté ?

En termes de répercussion internationale, l'affaire Snowden et les révélations de l'été 2013 concernant les programmes de surveillance américain PRISM et XKeyscore, n'ont fait qu'accentuer un processus de régionalisation des *data centers*, processus initié dès la fin des années 2000. En effet, avant même qu'éclate le scandale, les gouvernements internationaux, que ce soit en Russie, en Chine ou en Europe, s'inquiétaient déjà de la domination des firmes américaines dans le domaine du *cloud computing*, et des conséquences stratégiques que ce rapport de force pouvait induire à moyen et long terme. D'où l'incitation des pouvoirs publics dans de nombreux pays pour voir se développer des *data centers* locaux et une offre de *cloud computing* permettant de faire contrepoids aux géant américains. En France, ce débat sur le « *cloud* souverain » a ainsi abouti ces dernières années à la mise en place des firmes Numergy (société fondée en 2012 à l'initiative de SFR et de Bull) et Cloudwatt (société fondée en 2012 par Orange en partenariat avec Thalès).

Il faut néanmoins rappeler ici les critères géographiques traditionnels qui pèsent sur la localisation des *data centers*, et qui doivent donc être pris en compte par les pouvoirs publics pour initier de tels projets. Il faut également noter que cette dynamique de régionalisation implique deux volets bien distincts, que sont :

- d'un côté, le développement d'entreprises nationales ou européennes, permettant l'émergence d'une offre « souveraine » d'un bout à l'autre de la chaine
- de l'autre, la régionalisation de l'offre déjà existante, avec la création par les géants du « cloud », de *data centers* localisés sur différents territoires partout dans le monde.

Aussi, la localisation des *data centers* n'est-elle pas à elle-seule un facteur totalement déterminant en termes de souveraineté et doit être remise en perspective avec ses différents paramètres pour pouvoir être appréciée en termes d'efficacité et de stratégie politique.

De fait, la localisation des *data centers* pour être optimale doit répondre à plusieurs facteurs géographiques. La présence d'une ou de plusieurs sources énergétiques fiables à proximité est primordiale. En effet, le fonctionnement d'un *data center* est particulièrement énergivore. IBM évalue que le coût énergétique d'un *data center* a été

multiplié par huit en dix ans[177]. Avec l'explosion des besoins, un *data center* de 10 000 m2 consommerait autant qu'une ville de 50 000 habitants, et ses besoins devraient tripler d'ici à 2020 [178] . Cette consommation énergétique est d'ailleurs nécessaire autant à son fonctionnement qu'à son refroidissement. D'où une localisation privilégiant un accès facilité à une source énergétique (à proximité d'une centrale électrique par exemple), ou dans des climats froids, facilitant le refroidissement des machines à moindre coûts (comme pour l'implantation d'un *data center* Google à Hamina en Finlande, motivé par la présence sur ce site d'eaux marines froides).

A ces premières contraintes géographiques s'ajoute la nécessité d'une implantation à proximité des points d'accès aux dorsales de l'Internet, pour assurer un débit fluide et permanent, et une accessibilité sans faille des données. La localisation d'un *data center* est donc à mettre en relation avec la géographie des nœuds des réseaux des opérateurs. La position de ces nœuds répond tant à un principe démographique (implantation dans des zones à fortes densités) qu'à un principe stratégique (en fonction des stratégies de développement régionales et internationales). Ces contraintes géographiques sont à prendre en considération dans le débat sur la possibilité d'un « *cloud* souverain », car elles conditionnent la construction d'infrastructures viables au niveau national et international. La souveraineté ici ne dépend pas seulement de la localisation sur le territoire national des infrastructures du *cloud*, et donc d'un contrôle supposé plus important de la chaîne de transfert des données, mais elle repose aussi sur l'efficacité réelle de ces structures et sur leur niveau de connexion au réseau.

Par ailleurs, il est important ici de distinguer deux types de régionalisation, que l'on peut désigner comme interne et externe. La régionalisation interne suppose la création d'une nouvelle offre montée par des firmes nationales ou européennes, et reposant en grande partie sur des infrastructures localisées sur le territoire étatique. Cette dynamique est le fruit des débats sur le « *cloud* souverain » initié dans les années 2000, et qui avait permis l'émergence de Numergy et de Cloudwatt en France. Toutefois, derrière ces gros projets industriels, on peut également mentionner des firmes plus réduites en taille, mais qui permettent d'élargir l'offre existante de *cloud computing* sur des secteurs spécialisés. C'est dans cet esprit que

[177] http://www-935.ibm.com/services/fr/fr/it-services/lautre-data-center.html (août 2014)
[178] Greenpeace (2012), How clean is your cloud ?, April, 52 p., http://www.greenpeace.org/international/Global/international/publications/climate/2012/iCoal/HowCleanisYourCloud.pdf

s'inscrit le plan « *cloud computing* », initié au sein les 34 plans industriels lancés en 2013 par le Ministre Arnaud Montebourg, et dirigé par Thierry Breton, PDG d'Atos, et Octave Klaba, PDG d'OHV. Parmi les parties prenantes de ce plan, on retrouve les principaux acteurs du *cloud* français à savoir Cloudwatt, Numergy, Jolicloud, ou les associations et syndicats professionnels Syntec Numérique, Afdel et Eurocloud. Le plan prévoit ainsi, à travers 10 propositions emblématiques[179], de développer et de promouvoir l'offre nationale en termes de *cloud computing*. De tels projets nationaux sont sans aucun doute nécessaires pour permettre à l'utilisateur d'avoir des alternatives à l'offre américaine. Néanmoins, ils n'ont pas pour le moment la même attractivité que l'offre des géants du secteur, qui disposent d'une plus longue expérience et d'un réseau d'infrastructures beaucoup mieux développé à l'international.

Aussi, face à l'émergence de ces divers projets nationaux, les principales firmes américaines ont-elles répliqué en proposant des offres régionales, créant une dynamique que l'on peut qualifier de régionalisation externe. Ainsi, dès 2012, IBM ouvrait un *data center* à Montpellier, ayant pour but de conserver sa clientèle française face aux nouveaux acteurs Numergy et Cloudwatt. Cette inscription dans l'espace européen participe d'une démarche mondiale puisque cette firme prévoit à l'horizon fin 2014, d'ouvrir 15 nouveaux *data centers*, portant le nombre de ses infrastructures à 40, dispersées sur la planète. Cette stratégie essaye de répondre également aux préoccupations de confidentialité, suite à l'affaire Snwoden, et se double de la création de firmes nationales répondant à la juridiction des pays dans lesquels IBM est implanté.

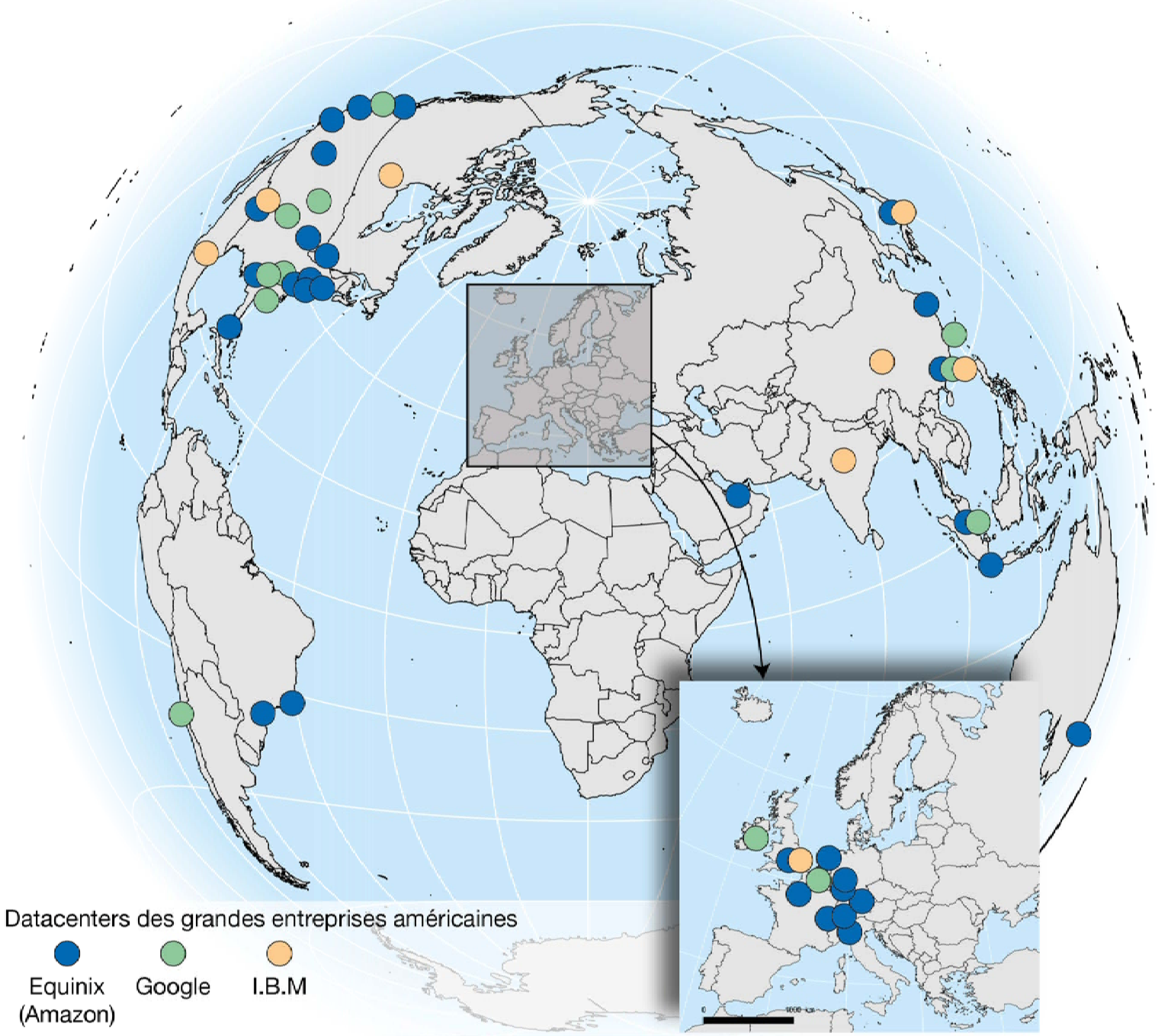
L'examen des politiques de développement d'Amazon Web Services ou de Google illustre des problématiques similaires, avec la volonté d'élargir leur offre et de proposer aux usagers des contrats permettant d'inclure une clause de localisation. Tout comme IBM, ces firmes tentent également de trouver des biais juridiques pour échapper à la contrainte du *Patriot Act*, et reconquérir la confiance de leurs clients internationaux. Par ailleurs, les infrastructures développées en Chine se plient aux exigences gouvernementales chinoises,

[179] Parmi ces propositions, on trouve l'idée de la création d'un label européen « Secure cloud », l'incitation par les marchés publics, à travers une politique « Cloud First », l'accompagnement de la transformation numérique des entreprises, la création d'un « espace de confiance européen », la mise en place de mesure concernant la localisation des données en France et en Europe, le soutien à l'innovation, la création d'un observatoire du Cloud, entre autres.

notamment en termes de censure[180], ce qui implique de la part de ses industriels un clair intérêt économique à respecter les clauses de souveraineté nationale des Etats, lorsque le marché en question est suffisamment important.

[180] http://www.zdnet.fr/actualites/pour-s-implanter-en-chine-amazon-se-plie-aux-regles-de-pekin-39167891.htm - août 2014

12. - Une infrastructure *cloud* principalement localisée aux Etats-Unis et en Europe



La notion de « *cloud* souverain » est donc ici à relativiser. De fait, la localisation des *data centers* et la création *ad hoc* de firmes nationales ne sont pas en soi des gages de souveraineté. Il est important d'examiner la qualité de l'offre proposée et de promouvoir la diversité des prestataires, seule à même d'instaurer un équilibre entre l'offre et la demande, entre les prestataires et les usagers. Celles-ci devraient amener les fournisseurs à proposer des offres plus souples et plus transparentes et à renforcer les gages en termes de sécurité et de localisation des données. De fait, les prestataires américains n'ont pas les mêmes intérêts que l'administration américaine et peuvent aussi s'inscrire dans des logiques de « souveraineté nationale » pour des pays étrangers.

3.4 Le *cloud* externalisé : les divergences d'intérêt entre prestataires et pouvoirs publics américains (L'exemple d'Amazon).

Le *cloud computing* est-il irrémédiablement voué à provoquer la fragmentation du web sous l'influence de réglementations visant à préserver la souveraineté des Etats qui auraient la volonté de s'opposer aux prétentions extraterritoriales du Droit américain ? Deux éléments de réponse permettent de répondre par la négative. Le premier tient à la politique des firmes dominantes dont l'intérêt bien compris est de ne pas apparaître comme les porteurs d'une politique de contrôle et de surveillance « impérialiste » des autorités publiques américaines. Le second tient à la distinction qu'il convient d'opérer entre la dimension technique du *cloud computing* (intégration des systèmes décentralisés) et sa dimension organisationnelle (externalisation de l'activité de traitement de l'information).

Comme on pouvait s'y attendre, les dirigeants de Microsoft ont réagi vigoureusement aux deux décisions judiciaires qui leur enjoignent de remettre les données dont ils sont dépositaires aux agences de renseignement américaines. En faisant reposer l'étendue du pouvoir de contrôle de l'administration sur la nationalité du dépositaire et non sur le lieu de stockage des données, les deux juges qui se sont prononcés sapent très directement la confiance des clients envers les opérateurs dominants, surtout dans un contexte où la méfiance est désormais solidement installée à la suite des révélations d'Edward Snowden. En renforçant le sentiment préexistant de méfiance vis à vis des opérateurs américains du *cloud computing*, ils remettent en selle une offre alternative, composée d'opérateurs nationaux ou locaux et qui s'étaient avérés jusqu'ici incapables de rivaliser techniquement et économiquement avec les firmes américaines dominantes.

Cet avatar judiciaire est l'occasion de souligner que la logique concurrentielle des opérateurs américains ne s'aligne pas sur la logique politique de leur gouvernement et qu'ils entendent offrir des garanties à leurs clients pour conserver un marché particulièrement sensible à la question de la sécurité des données informatiques. Il apparaît ainsi que l'intérêt bien compris des prestataires de service est de donner toute garantie susceptible de construire ou de maintenir le lien de confiance sans lequel il n'est pas de *cloud computing* possible, ce qui suppose le cas échéant de prendre des mesures visant à échapper à une interprétation extensive du Droit américain. Dans le même esprit, Amazon Web Services encourage très fortement ses clients à procéder à un chiffrement solide de leurs données confidentielles de sorte à les rendre inaccessibles au dépositaire lui-même.

Le *cloud* ainsi proposé par les prestataires de service américains se rapproche d'une sorte de « coffre fort numérique », dont le contenu peut être mis en forme, localisé et relié au réseau global selon les directives voulues par le client. Reste la question de l'obligation faite aux opérateurs américains de fournir aux agences de renseignement les informations détenues sur des clients étrangers et qui seraient stockées hors des Etats-Unis. On notera que les deux jugements rendus jusqu'ici le sont par des juridictions intérieures et que les voies d'appel permettront de reposer la question de l'équilibre entre les nécessités de la défense et de la sécurité nationale et la compétitivité de l'offre des entreprises américaines les plus innovantes. Il n'est pas certain que la pression de ces dernières ne finisse pas par conduire à une application moins ambitieuse des règles en vigueur aux Etats-Unis.

3.5 Le *cloud* internalisé : les conditions d'un contrôle poussé sur les données informatiques. (L'exemple de l'US Army)

Le *cloud computing* est très généralement présenté selon une approche globale au sein de laquelle on ne distingue pas ce qui relève de la réponse technique (l'intégration des matériels informatiques décentralisés) et du choix organisationnel (l'externalisation de la gestion du système ainsi intégré au profit d'un prestataire extérieur qui dispose des infrastructures, des ressources matérielles et des compétences pour offrir un service de qualité). Mais, ces deux dimensions ne sont pas indissociables et il est tout à fait possible de les envisager séparément de sorte à mettre en œuvre la solution technique au sein même des services de l'organisation concernée. Ce cas de figure, le *cloud computing* sans externalisation, revient à « faire soi-même » plutôt que de « faire faire ». L'organisation qui arbitre en ce sens ne bénéficie alors pas des avantages liés à l'agrégation des différentes

demandes individuelles que peut réaliser une firme extérieure spécialisée comme Amazon Web Services. Mais, elle en retirera tous les avantages liés au progrès technique et à la réorganisation de son système informatique proprement dit : rationalisation du parc de matériels et de logiciels en fonction des besoins des utilisateurs, recours à des matériels dont le niveau de performance unitaire est moins élevé, homogénéisation des solutions mises en place (par exemple, diminution de la diversité des langages informatiques autorisés dans l'organisation, unification des versions des logiciels déployés), renforcement de la sécurité des processus (mises à jours uniformes, disparition des interventions individuelles sur les matériels mis en œuvre…)

C'est le choix qui a été retenu par l'US Army. Celle-ci considère que ses informations sont souvent trop sensibles pour être confiées à un partenaire extérieur, fût-il une entreprise américaine notoirement liée à la Défense comme le sont les quatre grands du secteur. Le chiffrement, solution mise en avant par Amazon Web Services pour garantir la confidentialité des données, est jugé par trop fragile. L'institution préfère manifestement faire reposer la confidentialité et l'intégrité de ses données sur un contrôle matériel direct, en particulier la mise en place de matériels et de logiciels soigneusement analysés ainsi que de règles d'accès strictement définies. Le *cloud computing* s'inscrit donc dans un cadre hiérarchique qui autorise un contrôle étendu et non intermédié des infrastrutures, des composants matériels, des applications et des personnels, le facteur humain étant par ailleurs considéré comme la principale source de vulnérabilité du système. Préférence est donnée à la possibilité de gérer le traitement des données par un mécanisme de coordination hiérarchique : ordres et directives à des personnels qui relèvent de la ligne hiérarchique au sein de l'institution militaire.

Il semble également que la possibilité de faire varier le curseur de l'intégration et de la décentralisation en fonction des besoins du moment soit un argument en faveur de la solution interne. Une solution de type « tout *cloud* » supposerait pour que l'accès aux ressources informatiques soit assuré que tout utilisateur distant soit en mesure de disposer à tout moment d'un accès à un réseau dont le débit serait suffisant pour permettre l'emploi de logiciels puissants, donc gourmands du point de vue des transmissions. Or les missions militaires se déroulent le plus souvent dans des contextes où les moyens de communication sont limités et où les unités font preuve d'une très forte mobilité. Il conviendra alors de compenser le risque de ne pas pouvoir accéder au *cloud* dans des conditions satisfaisantes par la dotation des unités concernées en matériels disposant d'une autonomie élargie. Un équilibre doit alors être

trouvé entre la solution du *cloud computing*, efficace si l'accès au réseau des unités peut être garanti comme dans l'hypothèse où elles sont stationnées dans leurs bases habituelles, et une solution de type décentralisé lorsque ces unités sont projetées sur des théâtres où les communications sont plus aléatoires. La nécessité de disposer d'une vision d'ensemble et de développer une compétence interne en matière de gestion d'un réseau complexe semble être une justification non négligeable de la mise en place d'un *cloud* interne.

Le cas d'étude du *cloud computing* nous permet d'avoir une vision nuancée d'une possible fragmentation du web. De fait, la revendication de souveraineté en termes d'infrastructure émerge sur la scène internationale dans les années 2000 en réaction à la domination quasi absolue des firmes américaines sur ce marché, et à la prise de conscience de l'avantage stratégique que ce rapport de force peut revêtir à moyen et long terme. Pour répondre à cette situation, des projets industriels nationaux et européens ont été lancés et ont permis de mettre sur pied une offre alternative. Celle-ci reste néanmoins minoritaire et moins attractive que l'offre des principaux prestataires américains. Il n'en demeure pas moins que l'existence de cette offre a permis de réduire en partie la dépendance des clients européens vis-à-vis de l'offre américaine. En retour, cela a pu inciter les géants du *cloud* à proposer des formules plus en adéquation avec le souci croissant de confidentialité et de souveraineté touchant la clientèle et les gouvernements européens. Plus qu'une offre 100% nationale, ce serait plutôt la diversité de l'offre qui serait gage d'une plus grande souveraineté.

La question de la « balkanisation », si on l'entend comme celle d'une fragmentation nationale des infrastructures, est donc à relativiser dans le cas du *cloud*, pour au moins deux raisons. D'abord, les offres « nationales » ne peuvent être viables qu'en s'inscrivant dans un projet de développement à l'échelle européenne et internationale. Ensuite, cette diversité d'offres devrait permettre à moyen terme de rééquilibrer la relation en ce domaine entre les Etats-Unis et le reste du monde, même si une inversion des rapports de forces technologiques à moyen terme est très peu probable.

Toutefois, quelque soit la nature de l'offre, la sécurité des données absolue semble être un leurre. L'exemple du *cloud* interne développé par l'US Army est loin d'être exceptionnel. Si la souveraineté passe par la sécurisation des données stratégiques, elle implique donc aussi

un investissement nécessaire pour l'acquisition d'infrastructures nationales, permettant d'assurer une complète transparence dans la localisation, le stockage, et le transit des données stratégiques. L'existence de telles infrastructures appelle à la mise en place d'une grille d'évaluation des risques acceptables en fonction du degré de confidentialité des données. Cet outil d'évaluation est absolument indispensable pour maintenir un équilibre entre la volonté de souveraineté et la nécessité d'un accès à des services et des échanges efficaces et rapides.