NNT : 2016SACLE009

THESE DE DOCTORAT
DE L'UNIVERSITE PARIS-SACLAY
Préparée à Télécom École de Management

ÉCOLE DOCTORALE N° 578
Sciences de l'homme et de la société (SHS)

Spécialité de doctorat : Sciences politiques

Par

Monsieur Saïd EL OUAZZANI

Analyse des politiques publiques en matière d'adoption du Cloud Computing et du Big data. Une Approche comparative des modèles français et marocain.

Sous la direction de M. Gabriel Périès, Professeur HDR, Télécom École de Management.

Thèse présentée et soutenue à Paris, le 10 Juin 2016

Composition du Jury :

Président du Jury :
M. Imed Boughzala, Professeur HDR, Télécom École de Management.
Rapporteurs :
Mme. Anne Cammilleri, Professeure HDR, Institut d'Études Politiques de Rennes.
M. Thibault de Swarte, Maître de conférences HDR, Télécom Bretagne.

Remerciements

La présente thèse constitue l'aboutissement d'un projet, certes personnel, mais qui n'aurait pu se concrétiser sans le concours de personnes désormais indissociables de son histoire, des personnes que je tiens à remercier ici pour m'avoir accompagné dans ce qui restera une de mes plus marquantes expériences intérieures.

Tout d'abord, j'exprime ma très grande reconnaissance à **Monsieur le Professeur Gabriel Périès**, qui a dirigé mes travaux avec attention, rigueur et bienveillance. Ses conseils, critiques et recommandations formulés ont soutenu la réalisation de ce travail. Je le remercie également de m'avoir donné le goût et l'envie de m'investir dans la science politique après mon diplôme d'ingénieur dans l'informatique et les télécoms.

Je remercie les personnes, en France et au Maroc, qui ont accepté de répondre à mes questions, dont les noms et titres de certains figurent en annexe. Ces entretiens ont constitué une source première d'informations. Rencontrer les acteurs des politiques publiques a permis d'appréhender de façon plus concrète les enjeux essentiels de notre recherche.

J'adresse mes très sincères remerciements à Mme. Anne Cammilleri, M. Thibault de Swarte et M. Imed Boughzala, membres du jury, qui ont accepté d'examiner ma thèse et se sont rendus disponibles pour ma soutenance.

J'adresse également mes sincères remerciements à l'école doctorale Sciences de la Société (SDS) et toutes les équipes du laboratoire LITEM (Laboratoire en Innovation, Technologie, Economie et Management) de l'école Télécom Ecole de Management.

Je souhaite enfin et surtout remercier ma famille , mon père et ma mère, mais également mes frères et sœurs, pour leurs encouragements et leur soutien indéfectible durant la rédaction de cette thèse.

Qu'ils en soient tous remerciés, ici.

L'école doctorale n'entend pas donner aucune approbation ni improbation aux opinions émises par cette thèse.

Ces opinions doivent être considérées comme propres à leur auteur.

Table des matières

Introduction 12

1. Contexte générale de recherche 12

2. Définitions préliminaires 15

a) Le Cloud Computing : définitions préliminaires 15

b) Le Big data : définitions préliminaires 19

c) Les politiques publiques : définitions préliminaires 22

3. Choix de l'objet de recherche 24

4. Enjeux politiques liés à l'objet de recherche 25

5. Hypothèse de recherche 28

6. Choix de l'approche comparative : France et Maroc 30

7. Méthodologies de recherche 32

a) Contexte 32

b) Positionnement épistémologique: Le paradigme positivisme 33

c) Approche qualitative et mode de raisonnement abductif. 35

d) Approche des représentations et des savoirs liés aux analyses des politiques publiques: .. 37

e) Démarche d'entretien : Entretien semi-directif 38

f) Démonstration à travers une Étude de cas 39

8. Notions mobilisées 42

a) Les relations internationales 42

b) Le dispositif chez Foucault trouve son origine dans la notion de cybernétique 43

c) Le rôle de l'ingénieur dans la construction de l'État moderne 44

d) La révolution cybernétique 47

e) Du cyberspace à la cybermenace 48

f) De la doctrine de la « sécurité nationale » à l'ère du Cloud Computing et du Big data 49

9. Questions spécifiques de recherche 51

a) Quelle transformation technicienne de la notion de l'État chez Weber 51

b) Quels rapports de pouvoir à l'ère du Cloud Computing et du Big data ? 52

c) Quel rôle pour les partis politiques dans la transformation numérique ? 53

d) Quelle cybergéopolitique à l'ère de Cloud Computing et de Big data ? 55

10. Annonce du plan 57

I. Partie 1 : Comprendre l'action publique à l'ère du Cyber-État 64

1. Chapitre 1 : Étude de cas : Le Cloud et le Big data au service de l'action locale 65

A. Introduction..... 65

a) Contexte 65

b) Qu'est-ce qu'une collectivité territoriale ? 66

c) Les réformes des collectivités 67

B. Gestion du budget des collectivités 68

a) Contexte 68

b) Problématique de notre étude : vers une cyberdémocratie locale ? 68

c) Acteurs engagés 69

C. Description des travaux..... 70

a) Méthodologie du travail : 70

b) Les objectifs recherchés 70

c) Description des résultats..... 71

D. Les conclusions de l'étude de cas..... 75

2. Chapitre 2 : Comprendre l'action publique à l'ère du Cyber-État 76

A. L'État et le numérique..... 76

B. De la construction du Cyber-État 79

a) Contexte 79

b) L'aspect géographique délimitée disparait dans le Cyber-État..... 79

a) L'aspect obéissance à l'autorité dans le Cyber-État..... 81

b) L'aspect de légitimité de la violence par le Cyber-État 82

c) Définition d'un Cyber-État..... 83

C. Champs d'intervention du Cyber-État..... 84

D. Les services à l'ère du Cyber-État..... 86

a) Secteur public à l'ère du Cyber-État..... 86

b) Service public à l'ère de Cyber-État..... 87

c) La fonction publique à l'ère du Cyber-État..... 89

E. Performance et modernisation à l'ère du Cyber-État 91

a) Qu'est-ce que la performance de l'État 91

b) Modernisation de l'État et les écoles des politiques publiques néo-classiques 93

c) Modernisation de l'État en France 94
d) Modernisation de l'État au Maroc 96

3. Chapitre 3 : Les politiques publiques à l'ère du Cyber-État 99
A. Eléments de définition 100
a) Vers une cyber-politique publique 100
b) Vers une analyse des cyber-politiques publiques 100
B. L'analyse des cyber-politiques publiques à travers l'approche séquentielle 102
a) Définition 102
b) Schématisation de l'approche séquentielle 104
c) Les limites de l'approche séquentielle 104
C. Les acteurs dans les cyber-politiques publiques 105
a) L'acteur dans un processus de décision 105
b) Les groupes d'intérêt comme acteurs : Exemple de Syntec Numérique 106
c) Acteur clés des cyber-politiques publiques en France 107
d) Acteurs clés des politiques publiques au Maroc 108
D. Vers une « *Uberisation* » des politiques publiques 111
E. Comprendre la cyber-politique publique à travers le cas « Uber » 112
a) Choix du cas de la plateforme « Uber » 112
b) Emergence du problème « Uber » 114
c) Mobilisation des taxis classiques 115
d) Médiatisation du conflit 116
e) Réponse politique 116
f) Lancement de la plateforme « Uber » au Maroc 117

II. Partie 2 : La société numérique à l'ère du Cyber-État.....120

1. Chapitre 1 : La société numérique à l'ère du Cyber-État 120

A. La vie en ligne à l'ère de Cyber-État 121

B. Identité numérique ou cyber-Identité.....124

a) Contexte 124

b) Expressivité..... 125

c) Intimité 126

C. Vie privée , Privacy et Sphère privée à l'ère du Cyber-État.....127

a) Contexte 127

b) Vie privée..... 127

c) Privacy 128

d) Le concept de « Privacy by design »..... 129

e) Sphère privée 131

D. La problématique de protection des données à l'ère du Cyber-État.....131

E. Les principaux textes réglementaires de protection des données personnelles 133

a) Contexte 133

b) La loi française 78-17 « Informatique et Libertés »..... 133

c) La loi marocaine 09-08 (BO n°5714 du 05-03-2009) 134

d) Lignes directrices de l'OCDE 136

e) Directives du Conseil de l'Europe 138

f) La directive européenne 95/46/CE..... 138

g) La directive européenne 02/58/CE..... 139

h) Le nouveau règlement européen de protection des données personnelles 140

F. France : Commission Nationale d'Informatique et des Libertés (CNIL) 143

1) Contexte 143

2) La loi Informatique et libertés 144

3) Les missions principales de la CNIL 146

4) La CNIL et la cybersurveillance 147

G. Maroc : La Commission Nationale de la protection des Données (CNDP) 149

1) Contexte 149

2) Les missions principales de la CNDP..... 149

3) Composition des membres de la CNDP:..... 150

H. Comparaison des champs d'intervention de la CNDP et de la CNIL 151

I. Travaux du groupe G29 152

J. Travaux de la Chaire Valeurs et politiques des informations personnelles 155

K. Initiatives de l'Association Quadrature du Net 157

a) Création de l'association 157

b) L'association et la cybersurveillance 158

2. Chapitre 2 : cybersécurité et cybersurveillance à l'ère du Cyber-État 159

A. Cybersécurité à l'ère du Cyber-État 160

a) Le cyberspace à l'ère du Cyber-État 160

b) De la construction d'une cybermenace 163

c) Cybersurveillance à l'ère du Cyber-État 165

d) Retour sur l'affaire Snowden 167

B. Souveraineté politique et cybersouveraineté à l'ère du Cyber-État 170

a) Contexte 170

b) La souveraineté dans son sens général et politique 171

c) Vers une cybersouveraineté 173

d) Vers une politique numérique souveraine 176

C. Ré affirmer l'État de droit à l'ère de la sécurité nationale et du Cyber-État 177

a) Contexte 177

b) La loi de programmation militaire 2014-2019 179

c) La loi anti-terrorisme 180

d) La loi relative au renseignement 181

e) Travaux du séminaire IHEDN - Jeunes –IDF: La loi de renseignement du 24 juillet 2015 ... 184

f) De la Sécurité nationale comme doctrine de l'État 191

3. Chapitre 3 : Cybergéopolitique à l'ère du Cyber-État 199

A. La gouvernance d'Internet à l'ère du Cyber-État 200

B. « La république des ingénieurs » au service du Cyber-État 204

a) L'Internet Architecture Board (IAB) 204

b) Internet Engineering Task Force (IETF) 205

c) World Wide Web consortium (W3C) 207

a) Internet Corporation for Assigned Names and Numbers (ICANN) 209

C. Développement des protocoles et assignation d'adresses Internet (IP) 213

a) Le mécanisme d'élaboration des protocoles 213
b) Gestion des adresses Internet : Internet Protocol (IP) 217
D. Rapport de pouvoir dans la gouvernance d'Internet 219
E. « Neutralité du Net » à l'ère du Cyber-État 221
a) Contexte : 221
b) Origines..... 221
c) Eléments de définitions..... 224
F. Les aspects géopolitiques de l'affaire Snowden 227
a) Rappel du contexte..... 227
b) L'ennemi n'est plus seulement la Chine..... 228
c) Vers une balkanisaton du Cyberspace 229

III. Partie 3 : Fondements techniques du Cyber-État 231

1. Chapitre 1 : Fondements techniques du Cyber-État : Internet 232
A. Développement de l'Internet..... 232
B. Le rôle de l'Internet au quotidien..... 234

2. Chapitre 2 : Fondements techniques du Cyber-État : Cloud Computing 236
A. Introduction.....236
a) Contexte 236
b) Emergence du Cloud Computing..... 237
c) Le Cloud Computing dans la littérature..... 239
d) L'approche du National Institute of Standards and Technology (NIST) 240
e) Approche NIST : Modèles de service..... 242
f) Approche NIST : Modèles de déploiement 244
g) Approche NIST : Caractéristiques des services..... 246
h) Etude de cas démonstrative: Adoption de Cloud Computing..... 247
B. Le Cloud souverain à l'ère du Cyber-État 249
C. Vers des référentiels de confiance dans le Cloud 251
D. Quel Cloud Computing pour l'État marocain ? 252
E. Plan industriel Cloud Computing 254
a) Contexte 254

b) Des mesures en faveur de la demande (pour les particulier) 254
c) Des mesures en faveur de l'offre (pour les industriels) 255

3. Chapitre 3 : Fondements techniques du Cyber-État : Big data.....256
A. Big data comme fondement technique du Cyber-État 257
a) Définition du Big data 257
b) Caractéristiques de Big data 258
B. La fonction de « Chief Data Officer » à l'ère du Cyber-État 259
a) Contexte 259
b) Définition de «data scientist» 260
c) Le rôle de «data scientist» dans le service public 264
C. Les outils techniques de Big data 265
a) Machine Learning 265
b) L'outil Hadoop 268
c) MapReduce 269
D. Plan industriel Big data 270
d) Contexte 270
e) La formation des citoyens du Cyber-État 270
f) Développer un écosystème des start-ups autour de Cyber-État 271
E. Mission Etalab et ouverture des données publiques 273

4. Chapitre 4 : Autres technologies comme fondement technique du Cyber-État 275
A. Internet des objects 275
B. Intelligence Artificielle 278

IV. Conclusion 282

V. Bibliographie 290

VI. Annexes.....304
1 Glossaire.....304
2 Tables des figures et tableaux 306
3 Liste des différentes définitions de Cloud Computing 307

4 Liste des personnes interviewées acceptant d'apparaitre sur notre annexe : 314

5 Liste des travaux réalisés.....314

5.1 Colloque : l'efficacité collective à l'ère numérique 314

5.2 Participation aux travaux de la chaire «Valeurs et politiques des informations personnelles» de l'Institut Mines-Télécom 314

5.3 Séminaire « Gouvernance de données : Nouvelle pierre angulaire de la relation client du secteur bancaire ?» 315

5.4 Séminaire « Décentralisation et vie privée : une voie européenne ? » 315

5.5 Forum MEDays Tanger (Décembre - 2014) 315

5.6 Séminaire « WebDays » - Université Blida Algérie 315

5.7 Autres séminaires 315

5.8 Formations suivies 316

5.9 Cours enseignés 316

5.10 Autres activités académiques 316

5.11 Article : Comment le Cloud peut-il booster la compétitivité des PME ? 317

5.12 Article: Data scientist, métier d'avenir ou simple « buzz marketing »? 322

5.13 La souveraineté à l'ère du Cloud Computing 325

5.14 Article: Quel rôle pour la DSI à l'ère de cloud: Centre de profit ou centre de coût ? 333

Introduction

1. Contexte générale de recherche

Le scientifique américain Leonard Kleinrock qui a participé à la mise en place du projet ARPANET[(1)] a déclaré en 1969 qu' *« Aujourd'hui, l'ordinateur est à son enfance. Comme ils grandissent et deviennent plus sophistiqués, nous allons probablement voir la diffusion de l'utilisation des ordinateurs servant les maisons et les bureaux à travers le pays comme c'est le cas pour l'électricité et le téléphone»* / «*as of now, computer is still in their infancy. But as they grow up and become more sophisticated, we will probably see the spread of «computer utilities» which, like present electric and telephone utilities, will service individual homes and offices across the country*»).

Cette idée selon laquelle l'informatique serait fournie de la même manière que l'électricité et le téléphone fut présente dans les esprits des inventeurs d'Arpanet puis d'Internet. Après 46 années, l'idée de Kleinrok est se réalise alors que 3,025 milliards de personnes sont connectés à Internet, soit 42% de la population mondiale. Parmi eux, 2,060 milliards d'inscrits sur les réseaux sociaux, soit 68% des internautes. Aujourd'hui, nous comptabilisons un taux de pénétration d'Internet de 86% au Canada, 80% aux USA, 83% en France (contre 78% en Europe de l'Ouest), 24% au Maroc (contre 18% en Afrique), 66% en Amérique latine et 12% en Asie du Sud[(2)].

D'autres chiffres confirment la position dominante que le numérique occupe et occupera dans les années à venir. En effet, le numérique représente 5,5% du PIB en France[(3)], 90% des emplois nécessitent ou nécessiteront des compétences numériques d'ici à trois ans[(5)] alors que 57% des entreprises déclarent que la transformation numérique est un axe stratégique à moyen terme[(4)]. Un constant, dominant soit-il, est confirmé par Michel Serres[(6)] qui considère Internet au même plan que l'imprimerie tant elle constitue une rupture dans l'histoire de l'humanité. Alors qu'Internet ouvre un nouvel espace public de coexistence, essentiellement politique. Ce dernier n'est pas un espace comme un autre ni un medium d'interaction : il est le nouveau lieu du pouvoir économique, social et particulièrement politique.

---

(1) ARPANET ou Arpanet (*acronyme anglais de « Advanced Research Projects Agency Network est* le premier réseau à transfert de données développé aux États-Unis par la DARPA (Agence pour les projets de recherche avancée de défense). Le projet fut lancé en 1969 et il est à l'origine de l'Internet d'aujourd'hui.

(2) Statistiques fournie par l'agence *We Are Social* pour 2015. Le rapport complet est disponible sur l'URL:*http://wearesocial.fr/blog/2015/01/digital-social-mobile-les-chiffres-2015/* , dernière consultation 23 Juin 2015 à 15h15.

(3) Etude du cabinet McKinsey, « Accélérer la mutation numérique des entreprises : un gisement de croissance et de compétitivité pour la France» , Novembre 2014.

(4) Etude du cabinet Roland Berger, Du rattrapage à la transformation : L'aventure numérique, une chance pour la France, Septembre 2014.

(5) Rapport de la Commission Européenne, Le défi numérique européen, Octobre 2013.

(6) M. SERRES, Petite poucette , Paris, Editions le Pommier, 2012.

De la même manière que les infrastructures physiques comme les routes, les ponts, les ports et les relais de poste, ont permis aux États d'organiser les territoires et de déployer une souveraineté politique, ce sont maintenant les technologies numériques comme le Cloud Computing, le Big data, les technologies mobiles, l'Internet des objets, *etc*, qui agencent les nouveaux pouvoirs en s'appuyant sur les lois récentes relatives à la sécurité et au renseignement.

Ainsi, comme le précise Michel Volle dans son analyse stratégique[(1)], la numérisation d'une nation détermine son rang et son influence dans la géopolitique mondiale. En effet, depuis les débuts de l'informatique dans les années 1960 puis l'émergence du Web2.0 et ses réseaux sociaux des années 2000 jusqu'à l'avènement de l'Internet des objets et le web 3.0 aujourd'hui, les États-Unis ont été les précurseurs dans le développement des innovations numériques à travers des investissements massifs soutenus par la puissance publique et qui se sont traduits par la domination actuelle des plateformes[(2)] Internet nord-américaines.

Cependant, les États-Unis ne sont pas les seuls à prendre cette position de « *leader* ». La Chine, de son côté, développe ses propres plateformes comme en témoigne le positionnement des entreprises numériques chinoises : sur les 50 premiers plateformes numériques mondiales, on y trouve 36 américaines, 11 chinoises et 3 russes. La Russie a également émergé sur la scène numérique internationale en devenant à partir de 2011 le pays d'Europe comptant le plus d'utilisateurs d'Internet. Ce pays a également pu développer ses propres plateformes pour limiter toute dépendance vis-à-vis les États-Unis.

Avec deux systèmes politiques différents, la Russie et la Chine ont réussi à mettre en place les piliers fondamentaux ; économiques et techniques ; pour une industrie numérique d'avenir. Les autres pays des BRICS : le Brésil, l'Inde et l'Afrique de Sud, ont emprunté le même chemin en mettant en place des politiques publiques pour renforcer leurs infrastructures numériques et jouer un rôle important dans le paysage numérique mondial.

Ce développement numérique mondial s'est accompagné d'une réelle volonté politique. Josèphe Nye[(3)] souligne à quel point le cyberspace est devenu un enjeu important pour les États. Cet espace virtuel devient progressivement le théâtre croissant de tensions et de rivalité. En effet, la géographie de cyberspace, ou la géographie d'Internet, est très changeante et tout peut disparaitre d'un simple débranchement d'un ou de plusieurs équipements réseaux, ce qui pourrait déclencher une éventuel cyberguerre.

---

(1) Voir «L'informatisation d'une nation détermine son rang et son influence dans la géopolitique », publié par Michel VOLLE sur le site de l'Institut Français D'Analyse Stratégique, Mars 2013, Dernière consultation 09 Juin 2015, à 12h.

(2) Une plateforme Internet fait référence aux applications informatiques disponibles sur Internet en mode Cloud Computing comme Facebook, Google, Amazon, Yahoo, etc. Nous utiliserons fréquemment ce terme pour faire référence aux applications informatiques disponibles en mode Cloud Computing.

(3) J. NYE, The Futur of the Power, Public Affairs, U.S.A, 2011.

La diffusion élargie des plateformes Internet comme Facebook, Amazon, Google, *etc*, ainsi que la généralisation des smartphones, ont radicalement transformé l'ensemble de nos activités quotidiennes : Transport, logistique, services, santé, *etc*. En effet, ces plateformes numériques sont accessibles en ligne via Internet. Elles sont disponibles dans le Cloud Computing avec accès possible de partout et à tout moment. Elles exploitent toute sorte de données collectées comme les informations personnelles, données GPS, historiques d'utilisations, *etc.,* afin d'améliorer le service fourni, mieux connaitre les utilisateurs et générer plus de bénéfice en utilisant des technologies de Big data. Les utilisateurs de ces plateformes accèdent aux applications à travers leurs téléphones mobiles intelligents (smartphones) ou par tablette. Cette accessibilité est largement facilitée par la baisse des prix de la téléphonie mobile ainsi que l'évolution des infrastructures réseaux de la fibre optique, de la 3G, de la 4G et du WIFI disponible par des relais gratuit et partout.

En terme de mode d'emploi, l'utilisation de ces plateformes nécessitent, dans la majorité des cas, l'ouverture d'un compte électronique qui est associé par la suite à l'appareil mobile de l'utilisateur et à une solution[(1)] Cloud Computing. L'objectif est de pouvoir utiliser les services proposés et collecter les données relatives à toute l'activité de l'utilisateur depuis son appareil mobile. Nous remarquons qu'à partir de ces différents éléments, le Cloud Computing, le Big data et les accès mobiles (par smartphone ou tablette) constituent un ensemble technique cohérent qui pousse la diffusion des plateformes numériques sur Internet. C'est ainsi que le numérique et ses applications font désormais partie de la vie quotidienne d'une majorité de citoyens français et marocains entre-autres[(2)].

Le numérique, comme moyen de domination, de pouvoir et de contrôle, est aussi un facteur porteur de mutations profondes de la société et d'opportunités décisives avec l'émergence d'une économie et d'une société digitale. Les pouvoirs publics français et marocains doivent accompagner ces mutations à travers des politiques publiques ciblées afin de faire du numérique et ses applications un outil essentiel de croissance et de compétitivité. Sa bonne utilisation permet de réduire le décalage habituellement remarqué entre le temps des évolutions technologiques, très rapide, et le temps d'élaboration des règles et des lois par l'État jugé dès lors très lent par rapport à la vitesse des changements provoqués par le numérique comme en témoigne le dernier conflit entre les chauffeurs de taxis et la plateformes Cloud Uber en France.

---

(1) Par exemple, l'utilisation d'un iPhone nécessite un compte iCloud, une solution Cloud Computing de Apple. Toutes les données de l'utilisateur disponible sur l'appareil mobile de type messages, contacts, historiques des appels, photos, …, sont par la suite récupérées par Apple d'une façon automatique via une synchronisation périodique avec le téléphone de l'utilisateur et le iCloud d'Apple. Il existe des mécanismes pour limiter ce fonctionnement mais il nécessite des compétences techniques.

(2) Comme nous le détaillerons dans la partie *(1.2)*, nous étudions le contexte français et marocain, et nous essayons de comparer à chaque fois les politiques publiques des deux pays.

2. Définitions préliminaires

a) Le Cloud Computing : définitions préliminaires

Le terme Cloud Computing a de multiples définitions. En effet, l'article intitulé *«A break in the clouds: Towards a cloud definition»*[(1)], paru en 2008, en recense déjà vingt-deux définitions (*Liste des vingt-deux définitions disponible en annexes*).

Dans un travail commandé par le National Institute of Standards and Technology (NIST), une agence du département du commerce extérieur des États-Unis, Mell et Grance définissent le Cloud Computing comme étant :

> « *Un modèle permettant d'offrir un accès simple, en tout lieu et à la demande, à un ensemble de serveurs informatiques configurables et partagés (par exemple : réseaux, serveurs, stockage, applications et services). Cet ensemble de ressources peut-être rapidement approvisionné et mis en service avec un minimum d'efforts de gestion et d'interventions du fournisseur*»[(2)].

Par la suite, un grand nombre d'auteurs ont essayé de retracer un historique des définitions propres au Cloud Computing. Ce travail a été principalement conduit par Vaquero (2008), Etro (2011), Alali et Chia-Lun (2012).

Le terme Cloud Computing a été utilisé pour la première fois par R.Chellappa[(3)], cependant, d'autres auteurs comme Sultan[(4)] l'attribuent plutôt à Eric Schmidt, PDG de Google.

Le terme « *Cloud »* nous vient à l'origine du monde des télécoms et permet de représenter des réseaux des télécommunications et des réseaux Internet. Il symboliserait le traitement des informations sans intervention humaine et sans que l'utilisateur ait besoin de savoir ce qui se passe exactement. Ce postulat est partagé également par Plouin (2011) et Sultan (2014). Pour illustrer ce constat et à titre d'exemple :

> *Un utilisateur envoie une requête sur un site web Internet, il reçoit en retour une réponse sous forme d'une information sans savoir exactement où cette information il a été stockée ni d'où il provient ni comment elle a été traitée*.

---

(1) M. VAQUERO, L. RODERO-MERINO, J. CACERES et M. LINDNER, *« A break in the clouds: Towards a cloud definition* », Revue Harvard Business Review, États-Unis, Octobre 2008.

(2) P. MELL et T. GRANCE, The NIST Definition of Cloud Computing, NIST, 2011, p.2.

(3) R. CHELLAPPA, Cloud Computing: emerging paradigm for computing, Informs, 1997.

(4) N. SULTAN, discovering the potential of cloud computing in accelerating the search for securing serious illnesses, International Journal of Information Management, 2014.

A partir de ce constat, le terme « *Cloud* » fait référence à deux notions principales :

- La première notion est le *réseau des réseaux : Internet*. Ce réseau considéré comme complexe et constitué de millions de connexions, le chemin emprunté par l'information est méconnue du côté du client (appareil émettrice du signal) et le serveur (machine hébergeant l'application) [(1)] ;

- La deuxième notion à laquelle renvoie le terme « Cloud » est celle de *la localisation du client et du serveur*. Cette dernière, la localisation, n'est pas importante dans un échange à travers le Cloud et elle ne se considère plus comme une contrainte technologique. Le « Cloud » reste donc un moyen de connecter un utilisateur client à un serveur d'application situé quelques parts dans le monde[(2)].

Pour certains auteurs comme Begin (2008), Buyya (2009), ou encore Abbadi et Martin (2010), la popularisation de Cloud Computing est due principalement à l'apparition le 25 août 2006 de l'offre d'Amazon Elastic Cloud Compute (EC2) qui permet aux entreprises d'externaliser toute la gestion de leur informatique dans les centres des données d'Amazon.

Pour reformuler en d'autres termes, le Cloud Computing se résume aux principes suivants:

- Une consommation des services à travers Internet. A titre d'exemple, les solutions de messagerie électronique comme Gmail, Hotmail, Yahoo mail, *etc* ;

- Une gestion abstraite du logiciel et du matériel informatique d'un point de vue client. Ce dernier se concentre sur son cœur de métier (vente, achats, construction, *etc*.) et sous-traite la gestion technique informatique à des tiers spécialisés ;

- Un libre accès aux ressources informatiques, via Internet, depuis n'importe où et à tout moment avec un paiement flexible selon la consommation ;

- Un accès via une interface Internet à partir d'un appareil dédié.

En France, la commission générale de terminologie et de néologie, dont la mission est de favoriser l'enrichissement de la langue française, définit le Cloud Computing comme étant un «*mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire*». Cette définition est apparue dans le journal officiel n°0129 du 6 juin 2010. Cependant, dans les débats français, le terme anglais « Cloud Computing » reste largement utilisé.

[(1)] G. PLOUIN, Cloud Computing : Une rupture décisive pour l'informatique d'entreprise, Paris, Dunod, 2011.

[(2)] H. KATZAN, On An Ontological View Of Cloud Computing, Journal of Service Science, 2010.

Nous avons recensé à travers notre travail de recherche une trentaine de définitions pour le Cloud Computing, nous les mettons à disposition en annexe. Cette liste des définitions est organisée par auteur et par date de publication.

Ainsi, à partir de cette revue, nous pouvons adresser une définition générale qui couvre l'ensemble des aspects de Cloud Computing avec l'ensemble des caractéristiques qui se croisent pour chaque définition:

- Le Cloud Computing favorise un modèle «*service*» pour les clients. Le fournisseur ne commercialise pas des composants mais plutôt un service prêt à être déployé (Plouin, 2011). Cette notion de service est présente systématiquement dans la totalité des définitions ;

- Le service fourni se déploie à travers Internet. Ce réseau est largement cité dans les définitions. Un réseau local pourrait être utilisé également mais cela reste marginal dans les définitions que nous avons trouvées. Les auteurs faisant référence à l'utilisation d'Internet dans leurs définitions de « Cloud Computing » sont - présentés ici dans un ordre chronologique d'apparition de leurs définitions - : Armbrust (2009), Chen (2010), Haag et Cuming (2010), Katzan (2010), Shivakumar et Raju (2010), Nabil Ahmed (2011), David (2011), Espadas (2011), Lin et Chen (2012), Duta (2013), Gupta (2013), Ye (2013), Sultan (2013), Waxer (2013), Oliveira (2014).

A travers ces ouvrages ainsi que l'ensemble des articles scientifiques et journalistiques traitant le Cloud Computing, nous avons remarqué que la définition la plus répondu est celle donnée par le National Institute of Standards and Technology (NIST)[(1)].

Le plus important dans ce qu'il apporte la NIST est la grille de lecture du Cloud qui suit, avec ces éléments:

- *Trois modèles de service* : Software as a Service (SaaS), Plateforme as a Service (PaaS) et Infrastructure as a Service (IaaS) ;

- *Quatre modèles de déploiement* : Public, privé, hybride et communautaire ;

- *Cinq caractéristiques* : des services à la demande, des services mesurés, une bande passante élevée, un partage des ressources informatiques, et une élasticité et une flexibilité des ressources.

---

(1) Le National Institute of Standards and Technology (NIST) est une agence du Département du Commerce des États-Unis. Son objectif est de promouvoir l'économie américaine à travers le développement des technologies numériques.

Le schéma suivant reprend les différents éléments du modèle développé par le NIST. Nous y reviendrons plus en détails à l'étude de Cloud Computing dans la *section* dédiée au Cloud Computing.

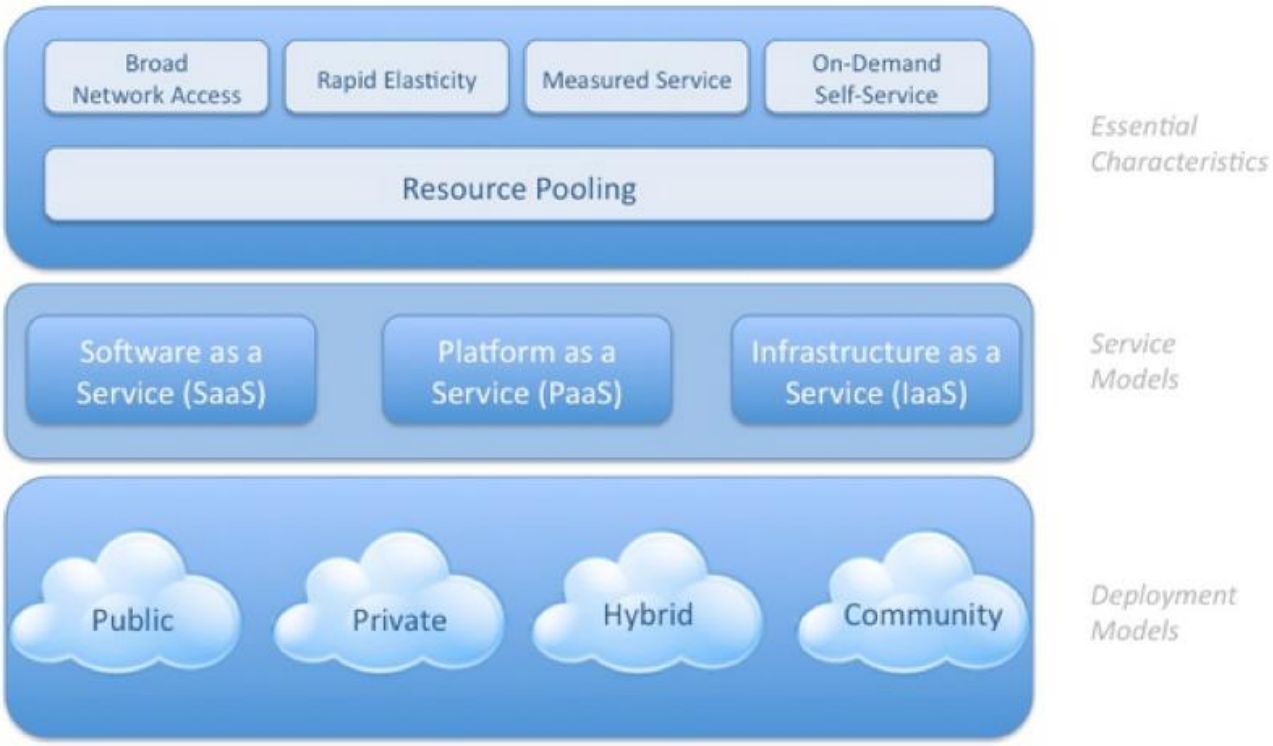


Figure 1 : Modèle de présentation du Cloud Computing par NIST

b) Le Big data : définitions préliminaires

Le terme Big data, traduit littéralement par « grosses données » ou « données massives », désigne l'explosion de la production des données à l'ère numérique.

Brynjolfsson et McAfee considèrent que le phénomène de Big data constituerait l'innovation de l'époque moderne[(1)]. Une innovation dont les effets impactent tous les domaines d'activités allant de la science et la recherche, en passant par le monde des entreprises, la gestion des services gouvernementaux et même le monde des arts[(2)].

Chris Anderson[(3)] considère que non seulement nos capacités à répondre aux questions fondamentales progressent à mesure que s'accroissent les faits, mais le Big data rendrait même obsolète la méthode scientifique traditionnelle.

Lev Manovich[(4)], en tant que représentant de l'école des humanités numériques[(5)], nous fait remarquer que le terme Big data est mal adapté. En effet, ce terme a été utilisé en sciences pour faire référence à des ensembles de données suffisamment grands pour nécessiter l'utilisation de superordinateurs, alors que de vastes ensembles de données peuvent désormais être analysés sur des ordinateurs de bureau en utilisant des logiciels standards.

La nouveauté du Big data ne réside pas seulement dans la quantité des données produites - mais aussi traitées - chaque jour par les individus, les organisations et les objets, mais plutôt en leurs capacités à être articulées à d'autres données en mettant en relation plusieurs bases de données[(6)]. En raison des efforts pour exploiter et agréger les données, le Big data est fondamentalement lié aux réseaux qui permettent aux jeux de données concernant un individu, des individus liés à d'autres, des groupes de gens, ou simplement concernant la structure de l'information elle-même, de s'interconnecter au sein d'un seul ensemble.

---

(1) E. BRYNJOLFSSON et A. MCAFEE, The Big Data Boom is the Innovation Story of Our Time, The Atlantic, 2011.

(2) The Economist, « Data, Data Everywhere. Special Report: Managing Information », 25 février 2010.

(3) Wired Magazine, Problem Of Theory, 16 July 2008.

(4) L. MANOVICH L, Trending: The Promises and the Challenges of Big Social Data, Debates in the Digital Humanities, ed M.K.Gold, The University of Minnesota Press, Minneapolis, 2011.

(5) Selon Le Petit Robert, Les humanités numériques sont un domaine de recherche, d'enseignement et d'ingénierie au croisement de l'informatique et des arts, lettres, sciences humaines et sciences sociales. L'anglicisme « humanités digitales » de l'anglais « *digital humanities* » est parfois aussi utilisé bien que l'adjectif « digital » désigne quelque chose « qui appartient aux doigts ».

(6) D. BOLLIER, The promise and perils of Big Data, the Aspen institute, 2010.

Pour caractériser un phénomène de Big data, nous avons remarqué une multiplicité de définitions souvent tournées vers le modèle des trois «V» : Volume, Vélocité et Variété. D'autres modèles «V» ont été développées par la suite pour prendre en compte toutes les caractéristiques du phénomène:

- *Volume* : la quantité de données générées va continuer à augmenter de manière exponentielle à l'ère des médias sociaux et des objets connectés ;

- *Vélocité* ou encore Vitesse : ces données massives sont générées de plus en plus rapidement et en flux continu. Leur analyse nécessite de plus en plus le temps réel ;

- *Variété* : ces données se présentent dans de différents formats (texte, image ou son, *etc*.). Ils peuvent être structurées, semi-structurées ou encore non-structurées ;

- *Variabilité*: ces données sont de nature variable c'est-à-dire elles peuvent être changeables et interchangeables au fil de l'eau ;

- *Véracité* : ces données entrant dans des cycles de traitement, leur qualité, authenticité et exactitude sont primordiales ;

- *Valeur* : celle-ci peut être tangible (monnayable) ou non mais toujours appréciable d'une manière ou d'une autre au regard de la performance organisationnelle.

Les champs d'application des technologies Big data sont multiples, on peut citer à titre exemple:

- Optimiser les interactions entre les distributeurs et leurs fournisseurs afin de bien réorienter les processus d'affaires[(1)] ;
- Offrir aux clients la bonne marchandise ou service au bon moment, au bon prix et par le bon canal de distribution[(2)] ;
- Mener en temps réel des expériences auprès des utilisateurs pour tester de nouveaux produits et services[(3)] ;
- Développer des outils de ciblage comportemental pour des fins publicitaires ;
- Analyser les traces laissées volontairement ou involontairement par leurs utilisateurs[(4)] ;
- Prédire quel sera le succès d'un bien culturel particulier avant, pendant ou après sa création[(5)].

---

(1) E. BRYNJOLFSSON et A. MCAFEE, The Big Data Boom is the Innovation Story of Our Time, The Atlantic, 2011.

(2) H. DAVENPORT, L. DALLE MULE et J. LUCKER, « Know What Your Customers Want Before They Do », Harvard Business Review, December 2011.

(3) H. CHOI et H. VARIAN, Predicting the Present with Google Trends, Keynote address at the Australian Conference of Economists, July 2011, Research Paper, 18 December 2011.

(4) L. GROSSMAN, « How Computers Know What We Want – Before We do », Time Magazine, 27 May 2010.

(5) H. DAVENPORT ET G. JEANNE, « What People Want (and How to Predict It) », MIT Sloan Management Review, 9 January 2009.

A partir de ces éléments, nous remarquons que les applications du Big data sont importantes. Cependant, il existe également des limites et plusieurs questions se posent :

- L'accès aux données est-il ouvert ou réservé à certaines entreprises spécialisées ayant les moyens financiers de les acheter, les rentabiliser, les exploiter et les analyser avec des outils et des mécanismes sophistiqués. Ces compétences sont loin d'être partagées par tous[(1)] ;

- Un nouveau «*digital divide*» est en train de se créer entre les «*Big data rich*» et les «*Big data poor*»[(2)].

Il existe également d'autres champs d'application de Big data pour des besoins de surveillance, de traçabilité et de reconfiguration du pouvoir. Nous y reviendrons plus en détails dans *la section* dédiée au Big data.

---

(1) L. MANOVICH L, Trending: The Promises and the Challenges of Big Social Data, Debates in the Digital Humanities, ed M.K.Gold, The University of Minnesota Press, Minneapolis, 2011.

(2) D. BOYD ET K CRAWFORD, Six Provocations for Big Data, presentation au symposium, "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society", Oxford Internet Institute, 2011.

c) Les politiques publiques : définitions préliminaires

i. Qu'est-ce qu'une politique publique

La politique publique capitalise déjà plus de quarante définitions en 1972. Thomas Dye en donne une définition simple, large en considérant que la politique publique est « *ce que les gouvernements décident de faire ou de ne pas faire* »[(1)].

De son coté, Lasswell mobilise le terme « *Policy* » (ou politique) pour désigner une décision importante dans ses travaux de « *Policy Sciences* ». Ainsi, l'usage de ce terme constitue pour Lasswell un moyen de définir un espace d'intervention de chercheur qui reste à distance des enjeux partisanes et du « *politics* »[(2)]. Par la suite, et peu à peu, il affine sa définition en considérant que la politique publique est un programme composé d'objectifs, de valeurs et de pratiques[(3)], et qu'elle est considérée comme un regroupement à la fois des valeurs, d'enjeux d'instruments, et de résultats pratiques[(4)].

Pour Jean-Claude Thoeing, «*Une politique publique se présente sous la forme d'un programme d'action gouvernementale, dans un secteur de la société ou un espace géographique* »[(5)]. Par la suite, avec Yves Mény, les deux auteurs considèrent qu'une politique publique «*se présente comme un programme d'action gouvernementale dans un secteur de la société ou dans un espace géographique».* Le programme d'action gouvernementale correspond à une *« combinaison spécifique de lois, d'affectations de crédits, d'administrations et de personnel dirigés vers la réalisation d'un ensemble d'objectifs plus ou moins définis*»[(6)].

Pour Patrick Hassenteufel: « *les politiques publiques correspondent à l'ensemble des actions de l'État. L'étude des politiques publiques est donc l'étude de l'État en action* »[(7)]. De manière similaire, pour Daniel Kübler et Jacques de Maillard, «*les politiques publiques sont au cœur du questionnement sur le mode de gouvernement des sociétés contemporaines*»[(8)].

---

(1) T. DYE, Understanding Public Policy , Englewood Cliffs N.J, PrenticeHall, 1972.

(2) H. LASSWELL et D. LERNER, The policy Sciences, Recent development in Scope and Method, Stanford University Press, 1951.

(3) H. LASSWELL et A. KAPLAN, Power and Society, A framework for Political Inquiry, London, Kegan Paul, 1952.

(4) H. LASSWELL, A Pre-View of Policy Sciences, New York, American Elservier, 1971.

(5) J-C THOENIG et Y. MENY, Politiques publiques, PUF, 1989.

(6) J-C THOENIG et F. DUPUY, L'administration en miettes Paris, Fayard, 1985.

(7) P. HASSENTEUFEL, Sociologie politique: l'action publique, Armand Colin, 2008, p.7.

(8) D. KUBLER et J. MAILLARD, Analyser les politiques publiques, Presses universitaires de Grenoble, 2009, p.8.

Les politiques publiques sont les programmes d'action qu'une autorité publique met en place dans un secteur de la société et dans un espace géographique afin de résoudre des problèmes publics[(1)] d'où se trouvent incluses évidemment les politiques sécuritaires. Il s'agit des résultats de décisions prises par des acteurs qui représentent la société. Dans une perspective centrée sur l'impact des actions du gouvernement, une politique publique peut être définie comme : « *Qui obtient quoi, quand et comment ?* »[(2)].

ii. Qu'est-ce qu'une analyse des politiques publiques

Le concept d'analyse des politiques publiques » (ou *policy analysis*), a vu le jour pour la première fois en 1930 aux Etats-Unis par Harold D. Lasswell[(3)] sans pour autant en donner une définition claire et précise. L'objectif à l'époque était de mettre en place une démarche d'analyse des politiques publiques afin de permettre à des analystes des projets du gouvernement fédéral américain de comprendre les choix politiques et aider les décideurs à en prendre les meilleurs et les plus pertinents.

Par la suite, dans la littérature des politiques publiques et pour qualifier ce qui est «d'analyse des politiques publiques », il existe une multitude de définitions. Pour Dunn par exemple, il définit le concept « d'analyse des politiques publiques » comme : «*Une discipline appliquée de la science sociale qui utilise de multiples méthodes de recherche et d'argumentation pour produire et transformer de l'information pertinente pour une politique, information qui puisse être employée dans des contextes politiques afin de résoudre des problèmes de politiques action*»[(4)].

Cette définition de Dunn est représentative de deux aspects fondamentaux de la discipline :

- Un caractère pluridisciplinaire de la démarche scientifique ;
- Une orientation vers une boite à outils d'aide à la décision et d'un savoir analytique.

Ainsi, analyser une politique publique consiste à étudier des aspects tels que la définition des problèmes publics, la prise de décisions, la formulation et l'évaluation. L'étude de ces éléments permet de déterminer à quel point l'activité du gouvernement s'approche de l'efficacité, et le niveau d'impact des décisions sur l'avenir et le bien-être général de la société.

---

(1) H. LASSWELL, A Pre-View of Policy Sciences, New York, American Elservier, 1971.

(2) J-C THOENIG et Y. MENY, Politiques publiques, PUF, 1989.

(3) H. LASSWELL, Psychopathology and Politics, Chicago (Ill.), University of Chicago Press, 1930.

(4) W.N. DUNN, Public Policy Analysis: An Introduction, EnglandWood Cliffs, Prentice-Hall, 1981, p.45.

3. Choix de l'objet de recherche

Le choix de notre objet de recherche et de l'approche comparative entre le modèle français et marocain était motivé par plusieurs raisons.

En effet, après nos études secondaires au Maroc, notre pays natal, nous avons pu constater que le rôle de l'État était essentiel dans le quotidien de la population. L'État central au Maroc est surnommé le Makhzen[(1)]. Ce terme renvoie à l'État marocain et ses institutions régaliennes. Le fonctionnement de ces dernières n'était pas connu du grand public marocain. Et c'est à partir de ce moment que nous avons commencé à questionner le fonctionnement de cette institution. Et depuis, nous avons porté un intérêt particulier pour les sciences politiques en générale et les politiques publiques d'une manière particulière.

Ensuite, nous sommes arrivés en France pour finaliser nos études d'ingénieur au sein de Télécom SudParis, une grande école d'ingénieurs de l'Institut Mines-Télécom. Cette école forme des ingénieurs généralistes dans le domaine des technologies de l'information et de la communication. Les élèves reçoivent au terme de leurs études le titre d'ingénieur diplômé de l'Institut Mines-Télécom.

Notre passage au sein de Télécom SudParis nous a permis d'acquérir des compétences techniques solides. Ces compétences techniques, analytiques et logiques sont nécessaires à la pratique du métier de l'ingénieur et à la compréhension des enjeux liés au numérique. En effet, nous avons eu une formation orientée numérique et axée sur les mathématiques, les télécoms et l'informatique dont le Cloud Computing et le Big data.

Ces compétences, nous ont permis de connaitre les architectures techniques et fonctionnelles de Cloud Computing, les différents mécanismes liés au Big data et maitriser les différents volets liés aux technologies mobiles.

A la fin de notre cycle d'ingénieur, nous avons intégré le cabinet du conseil parisien Accenture. Le cabinet Accenture accompagne les entreprises privées et les administrations publiques dans leur transformation numérique et la mise en place des solutions Big data et Cloud Computing. Au sein de ce cabinet, nous avons eu l'opportunité de participer à des missions d'accompagnement auprès de différents clients dont les administrations publiques comme le ministère des finances par exemple. Cette expérience nous a permis de mettre en pratique les connaissances acquises pendant le cycle d'ingénieur et de comprendre les enjeux et l'impact réel des technologies sur le fonctionnement des entreprises et des administrations publiques.

[(1)] Le terme « Makhzen » en arabe désigne littéralement « magasin ».

Notre connaissance des technologies étudiées à travers notre formation de base de l'ingénieur et sa mise en pratique à travers le métier du conseil ainsi que l'intérêt personnel porté aux politiques publiques, nous nous sommes décidés à nous lancer dans ce projet de recherche qui - à la fois - va nous permettre de :

- Satisfaire notre curiosité intellectuelle et comprendre le fonctionnement des administrations publiques française et marocaine ;
- Conjuguer nos différents champs d'expertises techniques et nos connaissance théoriques autour du numérique et de la science politique ;
- Notre culture franco-marocaine nous a motivé de partir sur une analyse comparative des deux modèles français et marocain.

Cette articulation pluridisciplinaire a donné naissance à ce projet de recherche qui va nous permettre de comparer les politiques publiques des deux pays en matière d'adoption de Cloud Computing et de Big data.

4. Enjeux politiques liés à l'objet de recherche

Si Machiavel était encore de ce monde, il ne manquerait pas de dire que dans notre société actuelle, la multiplication des princes de la Renaissance a entraîné une croissance du nombre de leurs conseillers. En effet, nous remarquons que les fonctions d'experts, de consultants et de chargés d'études autour des politiques publiques connaissent un développement considérable et se déploient à tous les niveaux. Mais qu'en est-il des politiques publiques destinées à analyser l'impact du numérique et plus spécifiquement de Cloud Computing et de Big data sur notre société contemporaine. Cet impact qui se matérialise à travers la transformation des liens sociaux entre individus, du pouvoir et d'autorité entre État et citoyen avec des programmes de surveillance de masse comme en témoigne l'adoption des lois récentes autour de la sécurité et de renseignement en France.

Les politiques publiques constituent au sein de la science politique et de la sociologie, une discipline qui couvre, par ses contributions, trois aspects : la connaissance, l'action et la formation[(1)]. En effet, « *les politiques publiques correspondent à l'ensemble des actions de l'État. L'étude des politiques publiques est donc l'étude de l'État en action* »[(2)] ou « *l'État en inaction* » si il décide de ne pas réagir.

[(1)] R. LANDRY, Introduction à l'analyse des politiques publiques, Québec, Presse de L'Université de Laval, 1980.

[(2)] P. HASSENTEUFEL, Sociologie politique: l'action publique, Armand Colin, 2008, p.7

Pour reprendre ces trois éléments dans le cadre de notre recherche, il s'agit alors de :

- Construire l'objet de recherche : Qu'est-ce qu'une politique publique en relation avec le Cloud Computing et le Big data ? Qu'est-ce qu'une souveraineté politique et numérique qui reposerait sur l'usage de ces techno-logies (*teknê-logos*)[(1)] ? Comment s'exerce le pouvoir du contrôle et de domination à l'ère de Cloud et de Big data ;

- Comprendre l'action de l'État en matière de politiques publiques. Cela revient à analyser les politiques publiques déjà adoptées ou en cours d'adoption et particulièrement les politiques publiques destinées au développement numérique ;

- Former les analystes des politiques publiques à comprendre les objets de recherche: les architectures techniques et fonctionnelles de Cloud Computing et de Big data. Ainsi, l'État peut disposer des compétences nécessaires pour accompagner la transformation numérique de l'ensemble des secteurs d'activités.

Ces trois notions ; connaissance, action et formation ; sont présentes en permanence dans les champs d'application et d'analyse des politiques publiques considérée comme «u*ne discipline appliquée de la science sociale qui utilise de multiples méthodes de recherche et d'argumentation pour produire et transformer de l'information pertinente pour une politique, information qui puisse être employée dans des contextes politiques afin de résoudre des problèmes de « politiques action » »* [(2)]. La vitesse de diffusion de l'analyse des politiques publiques au sein des différentes nations s'est révélée variable, et étroitement liée à la structure de l'État comme aux modes de raisonnement sur les affaires publiques lui correspondant[(3)].

Le numérique, dont le Cloud Computing et le Big data en constituent des piliers, est considéré comme un vecteur majeur de transformation des politiques publiques voire un enjeu de souveraineté politique et de sécurité de l'État. Pour relever ses nouveaux défis, les pouvoirs publics doivent anticiper l'ensemble des mutations de la société, retisser les liens entre l'État et ses administrés et favoriser la participation des citoyens à l'élaboration et au contrôle des politiques publiques à l'ère de la révolution cybernétique[(4)].

---

(1) Nous abordons la notion de « *teknê-logos* » dans la partie (*9.a) Rôle de l'ingénieur politique*

(2) W.N. DUNN, Public Policy Analysis: An Introduction, EnglandWood Cliffs, Prentice-Hall, 1981, p.45.

(3) P. DURAN, Penser l'action publique, Paris, LGDJ, coll. « Droit et Société », série «Politique », 1999.

(4) N. WIENER, The Human Use of Human Beings, 1950.

La diffusion des technologies numériques auprès de grand public impose au pouvoir public de s'interroger sur son mode de fonctionnement actuel ainsi que ses pratiques internes de contrôle afin d'assurer la sécurité et la souveraineté de l'État. Le numérique soulève donc de nouveaux enjeux à la fois pour la création et pour l'application du droit sur le territoire national où domine la raison de la décision, ou la cyber-décision. La territorialité de l'autorité souveraine est en effet remise en question par le caractère dématérialisé et transfrontalier des nouveaux usages avec l'émergence du Cloud Computing et du Big data.

Cette absence de frontière dans l'espace numérique s'accompagne aussi avec une absence des barrières techniques et réglementaires et commerciales voir même, sécuritaires. En effet, la souveraineté politique des États est remise en question depuis la révélation par Snowden du vaste système d'espionnage/intelligence mis en place à l'échelle planétaire par la NSA, l'Agence nationale de sécurité américaine via les affaires SIWIFT et PRISM[(1)], etc, dans le cadre de l'application de la loi Patriot Act[(2)] mais aussi par les lois récentes relatives à la lutte contre le terrorisme et sur le renseignement en France. Nous y reviendrons en détail dans *la section* dédiée à la cybersurveillance au sein du Cyber-État.

D'un point de vue économique, le numérique est omniprésent dans les négociations en cours entre les européens et d'autres nations comme l'accord entre l'Union Européenne et la Corée du Sud (déjà adopté), l'accord dit « CETA » avec le Canada (conclu mais non encore signé) et les deux projets de partenariats transatlantiques de commerce et d'investissement, « dit TTIP »[(3)] et « TiSA »[(4)], en cours de négociation avec les États-Unis.

---

(1) Acronyme de la Society for Worldwide Interbank Financial Telecommunication qui renvoie à l'autorisation donnée en 2007 aux USA par l'UE de contrôler l'ensemble des transactions bancaires qui transite par cette plateforme en entérinant des pratiques existantes depuis 2002 dans le cadre de la lutte contre le terrorisme. SWIFT gère près de 2 milliards de transactions par mois (2010). L'affaire PRISM renvoie à la découverte de ce réseau d'espionnage de la NSA dénoncé par E. Snowden en 2013.

(2) USA PATRIOT Act : Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (unir et renforcer l'Amérique en fournissant des outils appropriés pour déceler et contrer le terrorisme). Texte législatif adopté le 25 octobre 2001 après les attentats du 11 septembre et qui a modifié quinze lois fédérales, en octroyant au gouvernement et à diverses agences gouvernementales (dont le FBI, la CIA, l'armée) des pouvoirs sans précédent, en les autorisant à faire irruption dans chaque aspect de la vie des citoyens. Inaugurant un nouveau régime fondé en majeure partie sur le secret d'État, il neutralise les contre- pouvoirs en vigueur dans le système gouvernemental en laissant le pouvoir administratif empiéter sur le Judiciaire. Cette loi fut à l'origine considérée comme une loi d'exception dont les dispositions devaient initialement durer quatre ans. En juillet 2005, le Congrès a rendu permanentes 14 des 16 dispositions du texte. Après une longue bataille parlementaire au cours de l'hiver 2005-2006, la plupart des moyens accordés aux forces de l'ordre ont été pérennisés.

(3) The Transatlantic Trade and Investment Partnership (TTIP) ou Le Partenariat transatlantique de commerce et d'investissement (TTIP) est un accord commercial en cours de négociation entre l'Union européenne et les les États-Unis afin d'avoir des espaces de libres échanges commerciaux.

(4) The Trade in Services Agreement (TiSA) ou l'accord sur le commerce des services (ACS) est un accord commercial négocié actuellement par 25 membres de l'Organisation mondiale du commerce (OMC), dont l'Union européenne (UE) qui vise à éliminer le commerce des services entre les différents États.

La présence du numérique au cœur de ces négociations s'explique principalement par le fait que l'économie numérique représente un potentiel en matière d'internationalisation de tous les types de réseaux anciens ou modernes : criminels, étatiques, financiers ou terroristes, etc. D'ailleurs l'économie classique vit une transformation de son ensemble dans le cadre de cette économie numérique où le Cloud Computing et le Big data jouent un rôle prépondérant et déterminant.

Le Cloud Computing et le Big data constituent donc un véritable levier de développement et de modernisation de l'action publique. Les pouvoir publics doivent définir des stratégies claires et élaborer des politiques publiques adaptées afin de maitriser la diversité des choix technologiques et tous les enjeux du pouvoir associé : économiques, politiques, sécuritaires, etc.

5. Hypothèse de recherche

L'objectif de notre recherche consiste en l'analyse des politiques publiques françaises et marocaines et leur adéquation avec le développement des technologies de Cloud Computing et de Big data. En effet, nous souhaitons analyser ce que les deux États – français et marocain – font ou ne font pas en matière d'adoption de ces technologies.

Ce sujet de recherche est apparu en nous intéressant au secteur de Cloud Computing et Big data en 2011. Au départ, il n'y avait pas encore d'acteurs français ni marocains adoptant ces technologies. Les débats autour du numérique, et autour de Cloud et de Big data en particulier, étaient réservés à une poignée de spécialistes et d'experts. Ces débats n'étaient pas encore médiatisés comme c'est le cas aujourd'hui.

Au quotidien, nous avons eu l'opportunité, à travers nos différentes missions du consultant au sein de cabinet Accenture, d'échanger avec les grands acteurs de l'industrie informatique et les fournisseurs des technologies de Cloud Computing et Big data comme IBM, HP, Accenture, SAP, etc. Egalement auparavant en tant qu'élève-ingénieur avec nos professeurs à l'Institut Mines Télécom/Télécom SudParis. Tous ces échanges et ces expériences nous ont permis d'appréhender le sujet et ses problématiques.

Les enjeux politiques, économiques, sécuritaires et sociaux du Cloud Computing et du Big data étaient fondamentaux et constituaient l'une des problématiques à laquelle il fallait apporter une réponse pour enrichir le débat autour de la transformation numérique et ainsi participer au développement de l'État français et marocain. Nous avons donc saisi cette opportunité pour nous intéresser aux différents travaux autour de l'État et autour des technologies étudiées : Cloud et Big data.

En effectuant des recherches autour des thématiques de Cloud Computing et de Big data, nous avons constaté que la littérature de la science politique qui associe ces technologies à l'organisation de l'État était quasi-inexistante. Cela est dû principalement à la jeunesse de sujet ainsi qu'à son aspect très technique. Cependant, plusieurs ouvrages autour des thèmes

comme le cyberspace, cybersécurité, cyberguerre et cyberdéfense, *etc*., nous ont permis d'aborder le fonctionnement de l'État à l'ère du Cloud Computing et du Big data qui, d'un point de vue technique, constituent les bases techniques de ces notions de « *cyber-quelque chose* ».

Pour nous aider à comprendre les technologies du Cloud Computing et du Big data, nous nous sommes appuyés également sur plusieurs ouvrages et travaux universitaires dans le domaine des sciences de gestion. En effet, il nous semble intéressant que les sciences de gestion abordent ces questions de Cloud Computing et de Big data en donnant un discours de légitimation à ces systèmes. Cependant, Il faut considérer ces références d'un point de vue critique vu que la grande partie de leurs discours apparaissent comme légitimateur de pouvoir dans ce champ d'étude comme le souligne Pierre Bourdieu[(1)]. En effet, Bourdieu précise qu'un champ se définit par des enjeux et des intérêts spécifiques irréductibles à ceux d'un autre champ. Ainsi, ce qui fait courir un scientifique n'est pas ce qui fait courir un homme d'affaire ou un ecclésiastique. Bourdieu rajoute qu'un champ est un espace dynamique où se jouent des rapports de force et de domination poussant l'évolution du champ concerné[(2)].
Nous retrouvons dans ces références des sciences de gestion du sens commun, au sens que lui donne William James[(3)], considéré comme non critique à l'étude de notre objet de recherche. En effet, la transformation de l'État suite aux nouvelles théories marque une rupture avec la notion de l'État considérée par Weber[(4)] comme une entreprise détenant un monopole : celui de la violence légitime, mais une entreprise tout de même... et sur un territoire déterminé, mais un territoire aujourd'hui en voie de dématérialisation dans le cadre de la révolution cybernétique.

---

(1) P. BOURDIEU, Les Règles de l'art. Genèse et structure du champ littéraire, Paris, Seuil, 1998.

(2) P. BOURDIEU, Les Règles de l'art. Genèse et structure du champ littéraire, Paris, Seuil, 1998.

(3) W. JAMES, Le pragmatisme et le sens commun, Sociétés, N° : 89, *0*3/2005.

(4) M. WEBER, Economie et Société, Pocket, Paris, 2003.

6. Choix de l'approche comparative : France et Maroc

Nos sociétés contemporaines connaissent une transformation profonde opérée par les technologies numériques. La France, comme le Maroc, ne sont pas à l'abri des impacts de cette transformation, au contraire, ils y sont au cœur: La France étant la deuxième puissance européenne et le Maroc est considéré un des pays connaissant une croissance économique soutenue.

Ainsi, dans un contexte en permanence transformation, les entreprises privées comme les administrations publiques des deux pays sont, de plus en plus, exposées aux différents enjeux associés au numérique. Plus encore, l'État doit jouer son rôle et accompagner cette transformation en mobilisant tous ses moyens possibles tout en pensant pouvoir réorganiser — ou maintenir—son monopole de la violence légitime. Nous estimons donc qu'il est important de traiter l'objet de recherche selon les deux contextes suivants:

a) Contexte français

La société française est une des sociétés les plus connectées au monde. En effet, selon INSEE, en 2012, trois personnes sur quatre résidant en France métropolitaine ont utilisé Internet au cours des trois derniers mois, contre seulement 56 % en 2007. La fracture numérique se réduit entre catégories sociales : Internet touche la quasi-totalité des cadres depuis 2007 ; quatre ouvriers sur cinq l'utilisent en 2012, contre un sur deux cinq ans auparavant.

Ainsi, le développement accéléré de l'internet mobile accompagne ces évolutions. D'après l'INSEE, en 2012, 40 % des personnes résidant en France ont déjà surfé sur Internet, en dehors de chez elles, *via* un ordinateur portable, un téléphone portable ou un appareil de poche, elles n'étaient que 10 % cinq ans auparavant (2005).

La création d'un secrétariat d'État dédié à l'économie numérique montre l'intérêt que le pouvoir politique porte aux enjeux numériques et à titre d'exemple, la Direction Générale des Finances Publique (DGFP) est considérée comme l'une des institutions publiques au monde à avoir mis à disposition des procédures de déclaration d'impôts sur Internet et à travers une application du téléphone mobile. A cela s'ajoute le lancement d'une politique industrielle destinée à créer des pôles de compétitivité numérique pour mobiliser les facteurs clés de la croissance de l'économie numérique.

La spécifié du contexte français réside dans cette pénétration profonde des technologies numériques dans le quotidien de la société. En effet, selon les dernières statistiques, 42 millions de Français se sont déjà connectés à Internet. Ces multiples éléments montrent l'importance de traiter le sujet pour le contexte français. Ainsi, il est primordial pour les pouvoirs publics français d'adopter des politiques publiques autour des technologies de Cloud Computing et de Big data afin de rester un champion européen et mondial dans ce secteur d'avenir.

b) Contexte marocain

Selon les estimations de la banque mondiale, en 2011, 51% des marocains se connectent sur Internet. Par conséquent, le Maroc est classé troisième sur 54 nations africaines en matière d'utilisation des technologies Internet. Selon une étude menée par Maroc Numeric Cluster en partenariat avec *Averty Market Research & Intelligence*, institut d'enquêtes et de sondages d'opinion, 53% des internautes marocains passent plus de 4h par jour sur Internet en utilisant à 66% un support mobile. Le Maroc est ainsi devenu l'un des premiers pays africains à avoir mis en place un processus de demande de passeport complètement en ligne et 52% des marocains déclarent avoir eu recours à ce service avec des retours très positifs.

A l'image de la France, le Maroc a créé également la première instance, dans le monde arabe mais aussi en Afrique, dédiée à la protection des données personnelles. En effet, CNDP (Commission Nationale de Protection des Données Personnelles)[(1)] créée en 2009 a pour objectif de s'assurer de la bonne utilisation des données personnelles des citoyens marocains. Cette institution marocaine fait partie du Groupe des Autorités Européennes de Protection des Données Personnelles (G29).

Comme c'est le cas en France, le numérique est rattaché à une institution ministérielle. Au Maroc, il s'agit du ministère de l'Industrie, du commerce, de l'Investissement et de l'Economie Numérique. Cette institution publique s'occupe d'élaborer des stratégies de développement des secteurs de l'industrie, du commerce, des technologies ainsi leur déclinaison en politiques publiques. Par ailleurs, les autorités marocaines doivent accompagner l'adoption des outils technologiques par les administrations mais également être en mesure de protéger les citoyens et la souveraineté du pays et ses institutions régaliennes.

Nous remarquons donc que le rôle des politiques publiques en matière de numérique est fondamental pour assurer une place dans les paysages des grandes nations de numérique. Malgré les différents efforts menés par les autorités publiques en France et au Maroc, le constat reste contraste et mitigé par rapport à d'autres pays. En effet, ce retard enregistré en matière numérique influencerait le positionnement de la France dans les rapports géopolitiques mondiaux.

Le développement des politiques publiques pour favoriser la diffusion de la culture numérique doit être une priorité pour les autorités des deux pays. Ce travail doit combiner des actions au niveau des différentes politiques publiques industrielles, fiscales, scolaire, sécuritaires, *etc.*, afin de développer une vision, une stratégie et des projets cohérents à long terme.

---

(1) Dans le cadre de nos travaux de découvertes de terrain, nous avons rencontré le président de la CNDP à Rabat et nous avons pu échanger pendant 2h autour des problématiques de protection des données au Maroc mais aussi des enjeux numériques dont le Maroc d'aujourd'hui fait face.

7. Méthodologies de recherche

a) Contexte

Cette étape de la formulation de notre problématique de recherche a été une étape fondamentale parce que l'objet de recherche est supposé guider la construction de notre méthodologie de recherche. Ainsi, au cours des différentes étapes, nous avons suivi une méthodologie axée sur les approches suivantes :

- Une approche des représentations et des savoirs liés aux analyses des politiques publiques ;
- Une approche de l'entretien pour explorer le terrain de recherche ;
- Une approche par étude de cas pour mesurer l'apport concret de l'objet de recherche.

Nous avons également mobilisé plusieurs théories dont voici les principales :

- La notion de *dispositif* chez Foucault [(1)] et son utilisation dans le discours des ingénieurs ;
- Le retour de l'ingénieur dans la gestion de l'État moderne ;
- Politiques comparées et approches comparatives : Nous avons comparé tout au long de cette recherche le modèle français, pays industrialisé, avec le modèle marocain, pays en voie de développement ;
- Les relations internationales pour comprendre l'intérêt des États à coopérer pour assurer la sécurité de cyberspace et assurer l'avenir de l'Internet.

Il s'agit donc ici de réaliser une rupture avec le sens commun, avec le réel et de briser les relations les plus apparentes qui nous sont familières. Notre objectif est d'analyser les nouvelles relations que l'on construit entre les nouveaux éléments à partir de nos recherches comme le souligne Bachelard : « *Face au réel, ce qu'on croit savoir clairement offusque ce qu'on devrait savoir*» [(2)].

Ainsi, dans la suite de cette partie, nous allons détailler ces multiples notions et clarifions nos choix et comment nous les avons mobilisés durant nos différentes recherches.

[(1)] voir principalement M. FOUCAULT, L'Ordre du discours, Paris, Gallimard, 1971, P. 88 et M. FOUCAULT, Surveiller et punir, Naissance de la prison, Paris, Gallimard, 1975, P.324

[(2)] G. BACHELARD, La formation de l'esprit scientifique, Librairie J Vrin, 2000, p. 14

b) Positionnement épistémologique

Pour chaque travail de recherche, il s'agit de se questionner sur la position épistémologique du travail de recherche. En effet, L'épistémologie est « l'étude de la constitution des connaissances valables » [(1)]. Elle propose de porter un regard sur le statut, la méthode et la valeur de la connaissance. D'autres auteurs, en se basant sur les travaux initiés par Piaget, ont conduit des recherches autour des réflexions épistémologiques de la connaissance, sur sa définition et sur sa valeur scientifique. Ces travaux ont été principalement conduits par Le Moigne[(2)], Perret et Séville[(3)], Giordano[(4)].

En tant que chercheur en sciences politiques, nous nous sommes inspirés des travaux réalisés autour des paradigmes épistémologiques menés par Giordano[(5)]. Nous signalons que ces paradigmes épistémologiques sont également traités dans la littérature par plusieurs auteurs comme Le Moigne[(5)], Usunier[(6)], Wacheux[(7)] ou encore Perret et Séville[(8)].

D'après ses travaux, Giordano propose les trois paradigmes suivants : le positivisme, l'interprétativisme, et le constructivisme. Les différentes caractéristiques de chaque paradigme ainsi que les différences entre les trois sont détaillés dans le tableau[(9)] suivant :

---

(1) J. PIAGET, Logique et connaissance scientifique, Paris, Gallimard, 1967, p. 6

(2) J.L LE MOIGNE, Les Épistémologies constructivistes, Que sais-je ? , Paris, PUF, 1995V.

(3) PERRET et G. SEVILLE, Fondements épistémologiques de la recherche, dans Coll. « Méthodes de recherche en management » sous la direction de R.A.Thiétart, Paris, Dunod, 2007, p. 13-33

(4) Y. GIORDANO, Conduire un projet de recherche. Une perspective qualitative, EMS, 2003

(5) J.L. LE MOIGNE, Les Épistémologies constructivistes, Que sais-je ? , Paris, PUF, 1995

(6) J.C. USUNIER, Introduction à la recherche en gestion, Paris, Economica, 1993

(7) F. WACHEUX, Méthodes Qualitatives Et Recherches En Gestion, Paris, Economica, 1996

(8) V. PERRET et G. SEVILLE, Fondements épistémologiques de la recherche, dans Coll. « Méthodes de recherche en management » sous la direction de R.A.Thiétart, Paris, Dunod, 2007, p. 13-33

(9) Y. GIORDANO, Conduire un projet de recherche. Une perspective qualitative, EMS, 2003, p 25

	Positivisme	Interprétativisme	Constructivisme
(i) Nature de la réalité (Ontologie)	La réalité est une donnée objective indépendante des sujets qui l'observent	La réalité est perçue / interprétée par des sujets connaissant	La réalité est une : ▪ Construction de sujets connaissant qui expérimentent le monde ; ▪ Co-construction de sujets en interaction
(ii) Relation du chercheur / Objet de la recherche (Epistémologie)	Indépendance : Le chercheur n'agit pas sur la réalité observée	Empathie : Le chercheur interprète ce que les acteurs disent ou font qui, eux-mêmes, interprètent l'objet de la recherche	Interaction : Le chercheur co-construit des interprétations et/ou des projets avec les acteurs
(iii) Projet de connaissance	Décrire, Expliquer, confirmer	Comprendre	Construire
Processus de construction des connaissances	Fondé sur la découverte de régularités et de causalités	Fondé sur la compréhension empathique des représentations d'acteurs	Fondé sur la conception d'un phénomène / projet

Tableau 01 : Position épistémologique et Paradigmes de recherche

A partir de notre lecture de la grille de Giordano, nous considérons que :

- Nous sommes réalistes. Nous estimons que le positionnement réaliste implique que la réalité est une donnée objective indépendante des sujets qui l'observent.
- La relation entre le chercheur et l'objet recherché est indépendante. En effet, en tant que chercheur, nous nous n'agissons pas sur la réalité observée.
- Notre projet de recherche consiste à décrire, expliquer et confirmer des processus fondés sur la découverte de régularités et de causalités.

A partir de ces éléments nous nous situons dans le paradigme du positivisme tel qu'il est ici déterminé.

c) Approche qualitative et mode de raisonnement abductif

En plus du choix de sa position épistémologique, le chercheur peut choisir une approche quantitative ou qualitative pour aborder son objet de recherche accompagné d'un mode de raisonnement déductif, inductif, ou abductif. Il existe une grille de lecture pour distinguer les deux approches quantitatives et qualitatives. Ces dernières sont détaillées dans le tableau[1] suivant :

	Approche quantitative	Approche qualitative
Explication	Visée explicative ; Se concentre sur les objets	Visée compréhensive ; Se concentre sur les sujets
Examen de la théorie	Test de théories que l'on cherche à confirmer ou infirmer ; Logique de vérification	Généralisation de concepts, de modèles ou de propositions théoriques ; Logique de découverte
Universalité / Idiosyncrasie	Pré existence de lois universelles ; Objectifs de généralisation des phénomènes observés	Description de l'individualité de certains phénomènes ; La connaissance est construite socialement
Cause et interprétation	Identification des explications causales, des corrélations et des lois fondamentales qui expliquent des phénomènes récurrents	Interprétation de la structure d'un phénomène et recherche de liens de causalité locale
Objectivité / Subjectivité	Le monde est une réalité extérieure ; L'observateur est indépendant de l'objet de recherche	Le monde est un construit social ; L'observateur est partie intégrante de l'objet observé
Réduction des données, analyse et interprétation	Les problèmes sont scindés en éléments simples ; Le contrôle des variables est effectué à priori ; Le contexte est posé ; Les données sont considérées discrètes.	L'analyse est réalisée en profondeur ; Le contrôle des variables est effectué a posteriori ; Le contexte est appréhendé ; Les données sont considérées riches.

Tableau 02 : Comparaison des approches quantitatives et qualitatives

En effet, nous remarquons que :

- Les approches quantitatives cherchent à mesurer, à quantifier des phénomènes en effectuant des traitements statistiques de données.
- Les approches qualitatives ont pour objectif « d'expliquer un problème dans son contexte, de manière globale, dans sa dynamique » [2].

---

[1] M.HLADY-RISPAL, La méthode des cas: application à la recherche en gestion, Paris, De Boeck Uni, 2012, p.28

[2] R.A THIETART, Méthodes de recherches en management, Paris, Dunod, 2007, p.4

A partir de la grille de lecture de Hlady-Rispal[1], notre démarche de recherche se positionne en tant qu'approche qualitative pour les raisons suivantes :

- Nous ciblons une visée compréhensive en nous concentrant sur les problématiques traitées ;
- Nous souhaitons généraliser des concepts et des théories ;
- Nous souhaitons interpréter la structure des problématiques traitées et rechercher de liens de causalités ;
- Nous nous considérons en tant qu'observateur comme partie intégrante de l'objet observé ;

Dans sa démarche de recherche, le chercheur doit réfléchir au mode de raisonnement à adopter pour produire de la connaissance. La littérature offre plusieurs choix : l'hypothético-déductif, l'induction, et l'abduction.

Avec notre positionnement épistémologique « positiviste», et notre approche qualitative, nous avons le choix entre le mode de raisonnement :

- Mode de raisonnement inductif : Ce mode de raisonnement implique une observation libre et sans préjugé des faits de la part du chercheur ? Ce mode vise à construire des connaissances nouvelles à partir de l'étude de situation empirique[2] ;
- Mode de raisonnement l'abductif nécessite des « allers-retours successifs entre le terrain empirique et les théories et concepts mobilisés pour appréhender les situations empiriques étudiées » [3] ;

A partir de ces éléments, notre démarche de recherche s'inscrit dans un mode de raisonnement abductif pour les deux raisons suivantes :

- Notre observation est libre. Notre revue de la littérature a influencé notre perception, a donné des indications sur les problématiques étudiées.
- Nous ne pouvions pas nous aventurer sur le terrain et aller échanger avec nos interlocuteurs sans une étude préalable et une maîtrise de la littérature sur les politiques publiques, le Big data et le Cloud Computing. A partir de notre revue de littérature et de nos allers-retours sur le terrain, nous avons reformulés des propositions et conclusions, ces dernières ne sont pas considérées comme indiscutables mais restent plausibles.

---

(1) M.HLADY-RISPAL, La méthode des cas : application à la recherche en gestion, Paris, De Boeck Uni, 2012

(2) M.L. GAVARD-PERRET, Méthodologie de la recherche en sciences de gestion : Réussir son mémoire ou sa thèse, Paris, Pearson, 2012

(3) M.L. GAVARD-PERRET, Méthodologie de la recherche en sciences de gestion : Réussir son mémoire ou sa thèse, Paris, Pearson, 2012

d) Approche des représentations et des savoirs liés aux analyses des politiques publiques

Notre recherche s'inscrit dans une perspective d'analyse des politiques publiques visant à saisir les enjeux et les modalités de l'intervention de l'État dans le secteur numérique. En effet, les théories des politiques publiques ont fourni une trame de méthodologies analytiques permettant d'articuler et de généraliser nos recherches et observations[(1)].

A partir des éléments vu plus haut autour du sens de l'expression *«politique publique»*, notre analyse est centrée sur trois éléments : 1) les lois et les normes réglementaires, 2) les institutions[(2)] ayant pour fonction de maintenir un état social et 3) les programmes gouvernementaux de recherche et de soutien à l'industrie du numérique.

Par ailleurs, nous partageons l'idée selon laquelle la décision ne constitue pas un moment unique identifiable dans le processus politique mais se présente comme une succession de choix progressivement intégrés et transformés lors du processus politique, de la formulation du problème à la mise en œuvre de la solution choisie.

Dans la perspective d'une approche des représentations et des savoirs, les politiques publiques agissent comme des «*matrices cognitives et normatives constituant des systèmes d'interprétation du réel, au sein desquels les différents acteurs publics et privés pourront inscrire leur action*»[(3)].

Les deux courants majeurs de cette approche, fondés respectivement sur les paradigmes[(4)] et les référentiels[(5)], ont en commun de proposer que les politiques sont façonnées par des valeurs et des principes généraux qu'elles contribuent, en retour, à affirmer dans l'espace social. Comme Pierre Muller l'a souligné, la construction d'une matrice cognitive relève d'un processus de pouvoir par lequel un acteur fait valoir ses intérêts au sein d'un champ au sens qui lui en donne Bourdieu[(6)].

---

(1) D. MARSH et G. STOCKER, Methods in Political Sciences, Basingstoke: McMillan Press, 1995

(2) V. TOUNAY, La sociologie des institutions : Une sociologie processuelle, PUF, 2011

(3) P. MULLER et Y. SUREL, L'analyse des politiques publiques, Paris : Montchrestien, 1998, p.47

(4) P. HALL, « Policy Paradigm, Social Learning and the State », Comparative Politics, 1993

(5) P. MULLER, B. JOBERT, L'État en action : politiques publiques et corporatismes, PUF, 1987

(6) P. BOURDIEU, Les Règles de l'art. Genèse et structure du champ littéraire, Paris, Seuil, 1998

Dans le cadre de notre sujet, l'approche des représentations et des savoirs a fourni une grille d'interprétation pertinente à trois niveaux :

- Tout d'abord, elle a servi de cadre pour analyser le processus de formulation du problème public. Elle a impliqué l'identification des acteurs qui parviennent à imposer leur « vision du monde » et construisent ainsi le sens de la politique qui véhicule un champ dont l'enjeu est la domination ;
- Mettre en évidence la vision normative véhiculée par les instruments de l'action publique ;
- Proposer une explication du changement politique comme résultant d'une transformation des représentations du pouvoir selon la notion de la révolution cybernétique de Wiener (*cf. le point 8.d) Révolution cybernétique de l'introduction*).

e) Démarche d'entretien : Entretien semi-directif

L'analyse des politiques publiques semble avoir recouru à la revendication d'un regard originale, car empirique[(1)]. Les analystes des politiques publiques ont proposé d'étudier l'État «au concret» et «en action», aujourd'hui, l'entretien permet la mise en pratique de cette posture et en est la technique privilégiée[(2)].

L'entretien est une interaction verbale où le chercheur interroge un ou plusieurs acteurs sur l'objet de sa recherche. Cet entretien peut être directif, semi-directif ou non-directif :

- Un entretien directif repose sur des questions précises et est adaptées à un mode de raisonnement hypothético-déductif ;
- Un entretien non-directif repose sur le fait de laisser l'interlocuteur s'exprimer librement sur un thème assez large, il est adapté à un mode de raisonnement inductif ;
- Un entretien semi-directif est une posture intermédiaire qui offre au chercheur la possibilité d'interroger l'interlocuteur sur des thèmes souhaités, tout en lui laissant un espace d'expression.

Dans le déroulement de notre projet de recherche, nous avons effectué des entretiens semi-directifs.

Après avoir élaboré notre guide d'entretien, nous avons pu apporter des améliorations à notre littérature à la suite des échanges que nous avons eus avec les acteurs du terrain.

---

(1) P. HASSENTEUFEL ET S. ANDY, Essoufflement ou seconde souffle ? L'analyse des politiques publiques à la française », Revue française de science politiques, 2002

(2) P. BONGRAND ET P. LABORIER, revue française des sciences politiques, 2005

Les apports de la littérature ont été fort utiles pour s'armer des connaissances et des notions autours des problématiques de recherches traitées. Nous avons abordé le terrain, à l'aide d'un guide pré-structuré avec des thèmes d'études et des questions générales issues de notre revue de la littérature. Les questions ont été affinées et précisées au fur et à mesure de nos échanges avec les acteurs.

Nous avons pu rencontrer **25 personnes réparties entre experts techniques, responsables politiques, décideurs publics, étudiants, chercheurs, consultants et chefs d'entreprises**. Les personnes interrogées sont réparties géographiquement entre la France et le Maroc[(1)].

A la fin de chaque entretien, nous transcrivons les échanges et les utilisons comme références dans notre recherche ou comme base pour d'autres entretiens. La liste complète des personnes interrogées est disponible en annexe. Certains ont choisi de rester anonymes, nous nous ne citons pas donc ni leur nom, ni leurs professions ou établissements d'appartenance.

f) Démonstration à travers une étude de cas

Selon Hamel[(2)], l'étude de cas peut être désignée comme une approche susceptible d'englober plusieurs méthodes et techniques de recueil de données (observation directe, analyse de contenu, enquête par questionnaires et entretiens), sans pour autant comporter un protocole méthodologique strict.

Ainsi, en référence aux travaux de W. Dilthey[(3)], A. Schutz[(4)], nous comprenons que l'objectif à travers une étude de cas est la compréhension, plutôt que la démonstration ou l'explication. Ainsi, Cette orientation implique de se à focaliser sur les faits, le réel et « le vécu » des acteurs afin de comprendre une politique en profondeur.

En regardant de près la littérature autour des études de cas, plusieurs auteurs comme Glasser et Strauss[(5)], Yin[(6)], Wacheux[(7)], Hlady-Rispal[(8)], Giroux[(9)], Miles et Huberman[(10)], insistent sur deux critères principaux à prendre en compte pour toute étude de cas :

---

(1) E. NEGRIER, L'analyse comparée des politiques publiques : Méthodes et principes vécus, De Boeck Sup, 2005

(2) J. HAMEL, Étude de cas et sciences sociales, Paris, Le Harmattan, 1997

(3) W. DILTHEY, Introduction aux sciences de l'esprit, Cerf, 1992

(4) A. SCHUTZ, Contribution à la sociologie de l'action, Editions Hermann, 2009

(5) B. GLASSER ET A. STRAUSS, The Discovery of Grounded Theory: Strategies for Qualitative Research, Aldine Transaction, 1967

(6) R. YIN, Case Study Research: Design and Methods, Sage Publications, 2003

(7) F. WACHEUX, Méthodes Qualitatives Et Recherches En Gestion, Paris, Economica, 1996

(8) M.HLADY-RISPAL, La méthode des cas : application à la recherche en gestion, Paris, De Boeck Uni, 2012

(9) N. GIROUX, «L'étude de cas », in GIORDANO Y. (Coord.), Conduire un projet de recherche: une perspective qualitative, Paris, EMS Management & Société, 2003.

(10) M. Miles et A. Huberman, Analyse des données qualitatives, De Boeck Supérieur, 2003

- L'objectif de la recherche ;
- La nature de la problématique.

Nous souhaitons donc à travers cette étude de cas mieux appréhender l'objet de recherche et les phénomènes qui en émergent.

Notre motivation pour le choix de l'étude de cas est liée principalement à notre question de recherche. En fait, nous souhaitons à travers cette étude montrer comment un outil à la fois disponible en mode Cloud Computing, c'est-à-dire accessible par Internet, qui traite des données sous forme de Big data et également disponible sur une application mobile puisse permettre une concrétisation des principes étudiés dans le domaine de l'analyse des politiques publiques.

Dans notre étude de cas, il s'agit d'une politique budgétaire d'une collectivité territoriale. D'un point de vue processus d'élaboration des politiques publiques, nous nous positionnons au niveau de « la mise en œuvre» suivant l'approche séquentielle d'analyse des politiques publiques (*cf. chapitre 3 de la première partie*). Ainsi, nous avons remarqué que des questions de type « *comment ?*» et « *pourquoi ?*» sont les plus adaptées à une étude de cas et nous avons essayé d'y répondre à travers les deux questions suivantes:

- *Comment* une collectivité territoriale peut mettre en place un outil de contrôle de son budget en mobilisant les technologies étudiées : Cloud Computing, Big data, et disponible sous forme d'une application mobile ?
- *Pourquoi* un outil de contrôle numérique peut améliorer la relation entre le citoyen et l'administration publique ?

Nous avons donc répondu à ces deux questions à travers notre expérience dans la mise en place d'une solution informatique en mode Cloud Computing tout en se basant sur des technologies Big data. Nous y reviendrons plus en détails dans le premier chapitre de la première pour détailler cette étude.

Cependant, le choix de l'étude de cas est primordial dans la compréhension de notre question de recherche. Aussi, la représentativité du cas sélectionné, puis de la généralisation des résultats doivent être prises en compte avant le choix du sujet de son étude. Ainsi, le choix de nombre de cas à traiter dépend de l'objectif du chercheur et de son objet de recherche. Deux cas de figures se présentent :

- Une étude de cas unique permet une compréhension plus fine d'un contexte spécifique. Une telle étude est adéquate pour les exemples extrêmes ou les opportunités d'accès aux recherches inhabituelles[(1)], et elle facilite également la validité interne[(2)].

[(1)] K. EISENHARDT ET M. GRAEBNER, Theory Building From Cases: opportunities and challenges, Academy of Management Journal, 2007

[(2)] R. YIN, Case Study Research: Design and Methods, Sage Publications, 2003

Une étude de cas multiples permet d'améliorer la validité externe de l'étude et de procéder à des comparaisons[1] et donc de mettre en évidence les régularités, au sens de Koenig[2], ou de réplication au sens[3].

A partir de ces éléments théoriques, notre objectif à partir d'une étude de cas est d'affiner notre compréhension de notre problématique de recherche et spécifiquement de répondre aux deux questions du « comment » et le « pourquoi ». Par conséquent, une étude de cas unique nous semble la plus appropriée à notre contexte.

Nous avons travaillé sur notre étude de cas sur plusieurs mois avec la ville de Denver aux États-Unis en partenariat avec deux organismes locaux[4]:

- *Engaged Public* est un organisme de conseil en politiques publiques à destination du gouvernement américain. Il est situé dans la ville de Denver dans l'État du Colorado, aux États-Unis.
- *CausesLabs* une association qui travaille sur des projets humanitaires avec un impact positif dans la société tout en utilisant les outils technologiques.

Les objectifs visés avec cette étude de cas sont multiples. En effet :

- Nous avons adapté un outil, appelé « *Balancing Act »*, qui permet le contrôle des budgets des collectivités territoriales au contexte français. Cet outil à destinations des citoyens permet de contrôler la gestion du budget des communes et des élus locaux. Nous avons travaillé avec la commune de Boulogne-Billancourt dans les Hauts-de-Seine. ;

- Permettre d'évaluer l'adoption des outils technologiques par la population et d'évaluer les degrés d'acceptation dans la gestion des affaires locales ;

- Evaluer les accès à ces technologies ainsi que les politiques de l'Etat dans la couverture des territoires par des infrastructures numériques.

Nous reviendrons aux résultats et à l'organisation de cette étude dans le premier chapitre de la partie 1 afin d'alimenter les différentes notions de notre travail de recherche.

---

(1) M. MILES M ET A. HUBERMAN, Analyse des données qualitatives, De Boeck Supérieur, 2003

(2) G. KOENIG « Production de la connaissance et constitution des pratiques organisationnelles», Revue de l'AGRH, n° 9, novembre, 1993

(3) R. YIN, Case Study Research: Design and Methods, Sage Publications, 2003

(4) Nos méthodes de travail et d'échanges avec les partenaires américains étaient sous forme de Conférences téléphoniques par Skype et un échange quotidien par mail. Nous avons également construit un espace collaboratif d'échange de documents produits

8. Notions mobilisées

a) Les relations internationales

L'histoire des relations internationales opère selon des cycles qui se voient se succéder des périodes de crises et des périodes de stabilité, qui généralement se traduisent respectivement par des périodes de guerre et de paix. Il arrive aussi que ces cycles laissent place à de rares périodes combinant à la fois la crise et la stabilité.

Ainsi, le système westphalien définit les concepts directeurs des relations internationales modernes à savoir : l'équilibre des puissances, l'inviolabilité de la souveraineté nationale et le principe de non-ingérence dans les affaires d'autrui. Ces principes gouvernent la politique des nations la mise en place de ce système. Lorsque ces principes sont respectés, le monde connait globalement une stabilité politique.

L'ordre westphalien, c'est à dire celui de l'équilibre et des rapports de forces, se voient remis en cause à l'ère de Cloud Computing et de Big data. Ainsi, les concepts directeurs cités ci-dessus ne sont plus respectés. En effet, nous avons remarqué qu'avec l'affaire PRISM(1), les États-Unis ont violé les souverainetés nationales de plusieurs nations à travers la mise en place des programmes d'écoutes et de surveillance des dirigeants politiques de ces pays. Cette ingérence dans les affaires d'autrui par les Etats-Unis constitue une coupure avec le système westphalien qui assurait le respect de la souveraineté de chaque pays dans un rapport de force équilibrée.

Aujourd'hui la plupart des observateurs perçoivent que le système de sécurité collective tel qu'il est incarné par les Nations Unies et avant elle par la Société des Nations, ne correspond plus aux nouveaux enjeux de pouvoir et de sécurité à l'échelle mondiale. En effet, avec des technologies de Cloud Computing et de Big data, les Nations-Unies, et d'autres organismes, n'ont pas la capacité ni les moyens techniques et financiers pour contrôler le respect des principes westphalien comme en témoigne l'affaire PRISM.

Ainsi, dans ce travail de recherche, les théories autour des relations internationales ont été mobilisées pour analyser les nouveaux enjeux de la constitution d'une nouvelle norme internationale, et plus généralement, de la coopération entre les différents États afin de:

- Assurer la continuité du respect des principes westphalien à l'ère de Cloud Computing et de Big data: Respect des souverainetés nationales et non-ingérence dans les affaires d'autrui.

---

(1) PRISM, également appelé US-984XN1, est un programme de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques. Ce programme relevant de la National Security Agency (NSA) prévoit le ciblage de personnes vivant hors des États-Unis10. PRISM est supervisé par la United States Foreign Intelligence Surveillance Court (FISC) conformément au FISA Amendments Act of 2008 (FISA).

- Assurer le concept de « *la neutralité du Net* » ;
- Mettre en place une législation commune pour le respect de la vie privée des utilisateurs ;
- Mettre en place des normes communes et internationales liées au traitement des données personnelles des citoyens de différents États ;
- Assurer la souveraineté politique de chaque État à l'ère de Cloud, et de Big data ;

Par la suite, nous avons essayé de répondre aux questions suivantes :

- Quelle nécessité pour les États de s'organiser afin de garantir un espace commun à tous à l'ère de la révolution cybernétique[(1)] ?
- Comment éviter une mono-polarisation potentiellement conflictuelle des systèmes numériques ?
- Quels sont les intérêts pour certains États de coopérer dans un contexte des rapports de domination et du contrôle et faire face à des programmes de surveillance comme PRISM, Patriot Act avec l'état d'exception instaurée après la crise de 11 septembre, ou/et les structures adoptées dans le cade de la Doctrine de la sécurité nationale *(cf. section 8.f) de cette introduction)*.

b) Le dispositif chez Foucault trouve son origine dans la notion de cybernétique

Michèle Foucault est souvent cité dans les débats liés au concept du *dispositif*. En effet, il a développé ce concept à partir de 1970 et principalement à travers les deux ouvrages « L'ordre du discours »[(2)] et « Surveiller et punir »[(3)].

Le concept de *dispositif* se veut comme outil pour analyser un rapport de force pour orienter un discours, une technique ou une idéologie : Une techno-logie. Ainsi, pour Foucault, le dispositif s'inscrit dans une relation de pouvoir, comporte du discours et du non-dit, implémente et construit un savoir. Par la suite, Giorgio Agamben[(4)] a repris la définition de Michel Foucault et l'a développée pour interroger ce qui lie nos modes d'existence à des dispositifs techniques. Simon Lemoine[(5)], quant à lui, a repris également ce concept à partir de la conception de Foucault. En effet, il souligne comment et pourquoi un sujet est littéralement produit par les dispositifs qu'il fréquente comme l'école, l'usine, la prison, *etc*.

---

(1) **N.** Wiener, « Cybernétics or control and communication in the animal and machine», 1948

(2) M. FOUCAULT, L'Ordre du discours, Paris, Gallimard, 1971, P. 88

(3) M. FOUCAULT, Surveiller et punir, Naissance de la prison, Paris, Gallimard, 1975, P.324.

(4) G. AGAMBEN, Qu'est-ce qu'un dispositif ?, Rivages, 2014.

(5) S. LEMOINE, Le sujet dans les dispositifs de pouvoir, Presses Universitaires de Rennes, 2013.

A travers notre recherche, et en constatant les transformations induites par le numérique touchant toutes les institutions, dont la prison et l'usine que Foucault considère comme des dispositifs propices à la surveillance et au contrôle, nous essayé de comprendre :

- Si cette transformation met un terme aux contenus et aux logiques des dispositifs tels qu'ils ont été analysés par Michel Foucault.
- Si il existe une spécificité des dispositifs actuels liée à ces changements provoqués par le numérique ?
- Si le dispositif au sens foucaldien trouve ses origines dans un espace cybernétique comme le définit Norbert Weiner[(1)].

Nous avons essayé à travers notre projet de recherche d'apporter des réponses à ses questions en analysant les rapports de pouvoir entre États mais également entre États et les grandes plateformes Internet qui sont soumises habituellement aux lois, donc à l'autorité, de l'État qui les hébergent. Nous considérons pertinent d'analyser ces rapports de force afin de comprendre les enjeux qui accompagnent le développement de l'infrastructure numérique mondiale et de l'avenir de l'Internet.

c) Le rôle de l'ingénieur dans la construction de l'État moderne

La naissance de l'État moderne vient d'un processus qui a conduit d'une domination traditionnelle à une situation de domination légale rationnelle. Ainsi, selon la conception wébérienne[(1)], le pouvoir politique joue un rôle de moins en moins important dans la gestion de l'État moderne. En effet, il est plus adapté que les bureaucrates se chargent de la gestion de cet État moderne ainsi qu'ils y approprient le pouvoir.

De ce fait, en France, les grands corps sont appelés à exercer de grandes responsabilités au sein de l'État. Ces hauts fonctionnaires sont principalement issus des écoles supérieures d'ingénieurs: Ecole polytechnique, écoles des ponts, *etc*. Au Maroc également, les conseillers du roi, chargés des missions au sein du cabinet royal, occupent des postent stratégiques au sein de l'administration publique marocaine et sont également issus des parcours académiques d'excellence : grandes écoles française et américaines.

Ces technocrates, français ou marocains, ont participé au développement de l'État moderne dans chacun des deux pays et ont permis l'émergence d'une *techno-démocratie* ou une *technostructure*. Ainsi, cela a permis la formation du lien entre « *Tekhnê* » et « *Logos* » comme nous allons le voir dans la suite.

[(1)] Nous reviendrons dans la partie *(8.d)* de l'introduction pour détailler la notion de la révolution cybernétique comme elle était développée par Norbert Wiener.

i. Qu'est-ce que la technologie : « Tekhnê » - « Logoï»

Selon Melvin Kranzberg, « *La technologie n'est ni bonne, ni mauvaise, ni neutre… L'interaction entre la technologie et l'écosystème social est telle que les développements techniques ont des conséquences environnementales, sociales, et humaines qui dépassent de loin les objectifs des appareils techniques et des pratiques elles-mêmes*. »[(2)].

En effet, selon le dictionnaire Larousse, Le terme technologie, de son origine grec « *tekhnologia* », renvoie à quarte significations suivante:

- Étude des outils, des machines, des procédés et des méthodes employés dans les diverses branches de l'industrie ;
- Ensemble des outils et des matériels utilisés dans l'artisanat et dans l'industrie ;
- Ensemble cohérent de savoirs et de pratiques dans un certain domaine technique, fondé sur des principes scientifiques ;
- Théorie générale des techniques.

En effet, ce terme désigne tout ce que pourrait être fait par des outils dans les différents secteurs d'activités : l'art, la science, la médecine, *etc*.

En regardant dans Le Petit Robert, nous remarquons que le mot « technologie » est emprunté au grec « *tekhnologia* » de « *tekhnê* » et « *logoï*».

En effet, Le terme « *tekhnê* » désigne l'action de la fabrication matérielle. Une action considérée efficace chez les grecs. Le terme « *logoï*», quant à lui, désigne des disciplines du savoir comme les sciences, les arts, *etc*. En effet, plusieurs disciplines portent le suffixe –logie comme technologie, sociologie ou musicologie. Cependant, Le « logos » en grec désigne un langage, une raison, un discours, un principe qui définit tous les principes, et pour certains « Dieu ».

Comme précisé par Gabriel Péries[(1)], le couple « *Tekné-logoï*» renvoie à la diversité des pratiques technologiques qui mérite d'être interrogée par la prise en compte des divers systèmes de représentation et des imaginaires qui se constituent à partir d'elles. Une telle variété nous incite surtout à admettre que la technique est toujours en prise avec des logoï.

Dans notre contexte de recherche, La « *tecknê* » trouve son « *logos*» dans le profil de l'ingénieur politique (ou du politique ?) qui fabrique des outils techniques et produit des connaissances ou des savoirs politiques.

[(1)] M. KRANZBERG, Technology and History: "Kranzberg's Laws", Technology and Culture, Vol. 27, No. 1986.

[(2)] M. WEBER, Le Savant et le Politique, La Découverte, 2003.

ii. De l'existence d'une ingénierie politique ?

Le terme ingénieur n'a pris sa forme actuelle que depuis la Renaissance. En effet, ce terme a connu une évolution depuis l'Antiquité avec des significations diverses selon l'époque et le secteur d'activité concerné.

Selon le livre blanc des Ingénieurs et Scientifiques de France, un ingénieur doit intervenir pour le développement responsable de l'humanité selon les axes suivants:

- Mesurer la réalité des faits et mettre en œuvre des techniques de suivi ;
- Concevoir et mettre en œuvre des solutions concrètes aux nouveaux problèmes rencontrés ;
- Accepter une modification en profondeur des pratiques du métier de l'ingénierie et de leur positionnement dans les processus décisionnels.

A travers la construction de notre objet de recherche, nous avons tenté d'apporter des éclairages sur la manière dont s'est recomposée l'articulation des enjeux politiques, économiques et sociaux dans un contexte de transformation numérique et ce d'un point de vue de l'ingénieur-politique-digital.

Comme ce fut le cas pour Saint-Simon, ingénieur et entrepreneur de travaux publics sous Louis XVI. Il s'est battu aux côtés de La Fayette dans la guerre d'indépendance des États-Unis. Par la suite, il a construit une nouvelle entreprise industrielle et fait fortune faite avant de se retirer en 1802. Cependant, en 1816, il déclare que « *le plus grand homme d'état serait celui qui trouverait le moyen de diminuer le plus possible les charges du peuple, sans faire souffrir le service public* »[(1)]. En effet, le rôle d'un ingénieur-politique dans l'analyse des politiques publiques consiste à poser une finalité, à évaluer les contraintes, y faire élection des solutions les plus avantageuses. Le but ultime, est de mettre en place des politiques publiques efficaces comme en témoigne le rôle de l'ingénieur militaire à travers l'histoire. Ce qui, par conséquent, répondra plus tard à la définition de ce que l'on peut définir comme une politique publique.

Pour cet effet, nous avons vu naitre en France des écoles dédiées à la formation des ingénieurs des grands corps qui sont des corps d'État de hauts fonctionnaires au sein de la fonction publique française et également le développement des écoles ingénieurs au Maroc au même modèle que les écoles françaises.

[(1)] G. PERIES et P-A CHARDEL (Coord), Politiques sécuritaire et surveillance numérique, Paris, Hermès, 2014.

d) La révolution cybernétique

Les technologies numériques sont porteuses du complexe militaro-industriel. Historiquement, les technologies numériques sont apparues autour des recherches menées et/ou financées par les militaires américains, dont le Département of Advanced Research Projects Agency (DARPA). Cette agence militaire américain a pu développer les premiers supercalculateurs et a pu mettre les fondements de l'Internet d'aujourd'hui à travers le projet ARPANET. C'est à partir de ce contexte que nous avons vu donc née l'idéologie cybernétique.

Dans son ouvrage « *Cybernétics or control and communication in the animal and machine*», Norbert Wiener définit la cybernétique comme étant la *« Science du contrôle et de la communication chez l'animal et la machine»*[(2)]. Pour Louis Couffignal, *« La cybernétique est l'art de rendre l'action efficace.»*[(3)].

En effet, Norbert Wiener, considéré comme le père de la cybernétique, s'est vu financer ses recherches par le DARPA en vue de mettre au point des canons anti-aériens. L'objectif de l'armée américaine avec ces travaux est de mettre en place des outils pour prédire l'avenir des objets. Ainsi Wiener a pu mettre en place les fondements de la cybernétique autour de la notion de la rétroaction qui sert à reproduire ce que Gilbert Simondon[(4)] nommait la «bonne forme», la structure posée comme initiale qui ne fait pas apparaitre les dimensions symbolique et politiques. Politiquement parlant, l'idéologie cybernétique consiste à reproduire des conditions existantes.

Comme nous la présente Wiener, La cybernétique est une science du contrôle des systèmes. Ces derniers peuvent être une société, un individu, un groupe d'individus, des réseaux d'ordinateurs, des machines, *etc*. Un système cybernétique peut être défini comme un ensemble d'éléments en interaction consistant à échanger les informations. Les ordinateurs et toutes les machines intelligentes que nous connaissons aujourd'hui sont des applications de la cybernétique[(5)].

Le Big data est un bel exemple d'une application cybernétique. Les technologies Big data permettent une analyse prédictive à partir d'un ensemble de données collectées. Elles permettent aux objets de se connecter – (On parle de l'Internet des objets ou Internet Of Things), donc de prédire les comportements des personnes et des objets. Cela revient, au final, aux objectifs initiaux des travaux de l'agence pour les projets de recherche avancée de défense (DARPA) et de Wiener.

---

(1) J-F TETU, Pierre Musso, Saint-Simon, l'industrialisme contre l'État. Paris, Éd. de l'Aube, 2010

(2) N. WIENER, « Cybernétics or control and communication in the animal and machine», 1948

(3) L. COUFFIGNAL, La cybernétique, Presses Universitaires de France (PUF), 1963

(4) G. SIMONDON, L'individuation à la lumière des notions de formes et d'informations, Million, 2005

(5) N. WIENER, The Human Use of Human Beings, Da Capo Press 1988

e) Du cyberspace à la cybermenace

Le cyberspace est un objet d'étude lié à une multitude de définitions dans les mondes universitaires et militaires[(1)] ou liés aux secteurs de la criminologie et de la sécurité nationale[(2)]. En effet, le cyberespace est considéré comme un environnement[(3)], un domaine[(4)], un théâtre d'opérations, un espace[(5)], un substrat[(6)] et un milieu ou un moyen[(7)]. Ainsi, ce terme est considéré stratégique pour plusieurs auteurs et souvent utilisé dans les négociations internationales.

Ainsi, pour Pierre Levy[(8)], le cyberspace est considéré comme étant l'univers des réseaux numériques, un lieu de rencontre et d'aventures, un enjeu des conflits mondiaux et des nouvelles frontières économiques et culturelles. Comme le souligne Alix Desforges[(9)], le cyberspace est un espace plus englobant et plus virtuel. Il est à la fois un monde virtuel, dématérialisé, sans frontières, anonyme, de libertés, de partage et de communication

En effet, la représentation d'un cyberespace comme étant un espace de liberté, et de promotion de la démocratie est omniprésent dans les discours normatifs. Cependant, le sentiment d'insécurité est permanent dans un environnement cyberspace. Ce dernier, cyberspace, est identifié par le Livre Blanc de la Défense et la Sécurité Nationale de 2013 comme un « *champ de confrontation* » et devient le terrain de conflits de cyberguerre et de cyberdéfense. En effet, des actions criminelles peuvent être commises à l'encontre des États et des entreprises mais également à l'encontre des simples citoyens. On parle alors de la cybercriminalité ou de la cybermenace. Comme le note Myriam Dunn Cavelty[(10)], l'utilisation massive du préfixe *cyber-* consiste avant tout à désigner une action qui se fait par l'usage *d'ordinateurs* (Cloud Computing) et des *algorithmes* (Big data).

---

(1) A. BAUER, Violences et insécurité urbaines, Presses universitaires de France (Puf), 2006

(2) D. BETZ et T. STEVENS, Cyberspace and the State, Toward a Strategy for Cyberpower, The International Institute for Strategic Studies, Routledge, Londres, 2011.

(3) R. HARKNETT, Leaving Deterrence Behind: Warfighting and National Cybersecurity, in, Journal of Homeland Security and Emergency Management, March 2010.

(4) J. CARR, Inside Cyber Warfare: Mapping the Cyber Underworld, O'Reilly Media, 2011.

(5) O. KEMPF, Introduction à la cyberstratégie, Economica, 2015.

(6) C. DEMCHAK, Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI), Center for Cyber Conflict Studies, US Naval War College, 2012.

(7) M. LIBICKI, Crisis and Escalation in Cyberspace, Santa Monica, Rand, 2012.

(8) P. LEVY, L'Intelligence collective : Pour une anthropologie du cyberspace, La Découverte, 1994.

(9) A. DESFORGES, Les représentations du cyberespace: un outil géopolitique, La Découverte, Paris, 2014.

(10) M. DUNN CAVELTY, *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Routledge, Abingdon, 2008.

Cependant, il est difficile d'identifier les cybermenaces dans un cyberspace. En effet, les mêmes techniques d'attaque pouvant être utilisées dans le cadre d'une cyberguerre (attaque d'espionnage par exemple) ou de simple acte de cybercriminalité (pirate des données bancaires par exemple). Ainsi, le Livre Blanc de la Défense et de la Sécurité Nationale (LBDSN) français de 2013 identifie trois types de cybermenaces :

- La cybercriminalité qui ne relève pas spécifiquement de la sécurité nationale: Ce type d'attaque vise principalement les particuliers et les entreprises privées. Il consiste à pirater des informations personnelles, de dérober des données bancaires, etc. ;

- Les tentatives de pénétration de réseaux numériques à des fins d'espionnage : Ce type d'attaque vise les entreprises et les administrations publiques et principalement conduit par des organisations étrangères. L'objectif recherché est d'espionner les communications et avoir accès à des informations confidentielles ;

- Les attaques visant le sabotage de systèmes d'importance vitale : Ce type d'attaque vise à déstabiliser le fonctionnement d'un État. Ils peuvent être considérés comme un acte de guerre. Ainsi, il s'agit d'une atteinte à la souveraineté du pays.

Pour finir, nous remarquons que le cyberspace et la cybermenace véhiculent plusieurs représentations et se voient renforcer avec l'arrivée des nouveaux outils comme le Cloud Computing et le Big data. Cependant, les différentes conceptions de cyberspace sont retranscrites dans les stratégies - militaires soient-elles - des États, qui, de plus en plus, s'approprient des compétences nécessaires pour développer leurs propres outils de cyberguerre et de cyberdéfense.

f) De la doctrine de la « sécurité nationale » à l'ère du Cloud Computing et du Big data

Comme nous pouvons le lire dans le discours fondateur de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI):

> «*Le Livre blanc sur la défense et la sécurité nationale publié le 17 juin 2008 retient, parmi les menaces principales pesant sur le territoire national, les attaques informatiques. L'usage généralisé des technologies de l'information et de la communication ainsi que l'utilisation croissante des réseaux dans le fonctionnement de la société, font de la prévention et de la réaction face aux attaques informatiques une priorité majeure de nos dispositifs de* ***sécurité nationale*** *»*[(1)].

[(1)] Rapport de Secrétariat Générale de la Sécurité Nationale, dossier de presse, Juillet 2011. Le rapport complet est disponible sur l'URL: *http://www.ssi.gouv.fr/uploads/IMG/pdf/ANSSI_Dossier_de_presse.pdf*, dernière consultation 02 Juillet 2015 à 11h15.

En effet, les cyberattaques constituent, entre-autres, une menace pour la sécurité nationale. Ce terme ; qui a été introduit en France avec la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ; ne fait pas l'objet d'aucune définition précise. Ainsi, comme le souligne Gabriel Périès[(1)], la notion de la sécurité nationale est loin d'être neutre et s'interroge sur le contenu de cette notion et que que la jurisprudence renvoie à l'article 8 de la Convention européenne de sauvegarde des Droits de l'Homme de 1950. Un constant confirmé par Marc-Antoine Granger[(2)] qui souligne que « *la sécurité nationale doit- elle être considérée comme un objectif de sauvegarde de l'ordre public ? Dans le silence du Conseil, une telle interprétation est trop hasardeuse ».* Cependant, ce concept de sécurité nationale, malgré son caractère flou, non précis et à contenu indéterminé, figure dans plusieurs lois suivantes :

- *La loi de programmation militaire (PLM)* adoptée en 2013, qui souligne dans article L. 241-2 - « *Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article L.242-1, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale* ». Ainsi, l'adoption de cette loi et précisément son article 20 manifeste une profonde crise d'un pouvoir politique n'hésitant plus à porter massivement atteinte aux droits fondamentaux sous prétexte des impératifs de la défense et la sécurité nationale ;
- *La loi anti-terrorisme n° 2014-1353* adoptée en 2014 consiste à renforcer la lutte contre le terrorisme et à prendre en compte les évolutions récentes des actes de terrorisme et spécialement ses aspects technologiques. Le texte renforce la répression de l'apologie du terrorisme et de la provocation à des actes pouvant atteindre la *sécurité nationale*. Cependant, Si la lutte contre le terrorisme est légitime surtout dans un contexte internationale mouvementé mais elle ne peut pas justifier de légiférer en urgence sans lancer des débats nationaux qui vont permettre à l'ensemble de la population : citoyen, experts, décideurs politiques, etc., de s'exprimer et éviter mettre en place des lois avec des graves atteintes aux libertés fondamentales ;
- *La loi n° 2015-912 relative au renseignement*, adoptée après les attentats de Janvier 2015 et validé définitivement le 24 juillet 2015, vise à donner un cadre légal pour les activités des services de renseignement, qui fonctionnent jusqu'à présent dans un cadre illégale, pour faire face à toute atteinte à la sécurité nationale. Les finalités de cette loi sont légitimes mais cette constitue une atteinte au respect des droits fondamentaux des citoyens sous prétexte de la sécurité nationale et représente un certain nombre de points inquiétants qui nécessitent un débat élargi.

Nous reviendrons en détail sur l'institutionnalisation de la sécurité Nationale comme doctrine d'État ainsi dans *la section 2 dédié à cet effet*.

---

(1) G. PERIES, La confiance au prisme de la « sécurité nationale». Une analyse critique à l'ère des réseaux numériques, Politiques sécuritaire et surveillance numérique, P-A CHARDEL (Coord), Paris, Hermès, 2014, P.59.
(2) M-A GRANGER, Constitution et sécurité intérieure. Essais de modélisation juridique, LGDJ, 2011, p. 83-84.

9. Questions spécifiques de recherche

a) Quelle transformation technicienne de la notion de l'État chez Weber

Selon Marx Weber, les fondements de pouvoir politique et les sources de sa légitimité justifiant la domination de l'État sur les autres gouvernés. En effet, Max Weber[98] définit l'État comme :

> « *Une entreprise politique de caractère institutionnel lorsque et en tant que sa direction administrative revendique avec succès, dans l'application des règlements, le monopole de la contrainte physique légitime […] Comme tous les groupements politiques qui l'ont précédé, l'État consiste en un rapport de domination de l'homme par l'homme fondé sur le moyen de la violence légitime* »[1].

Ainsi, la conception wébérienne de l'État repose sur quatre éléments fondamentaux :

- Tout d'abord, l'État est un *espace géographiquement délimité* ;
- Au sein de cet espace géographique, le caractère institutionnel introduit l'idée de rapports *d'autorité à obéissance* ;
- Ces rapports d'autorité à obéissance au sein de l'espace géographique de l'État sont supposés être *pérennes et durables* ;
- Dans cet espace géographique, l'État a le *monopole de la légitimité*.

Cependant, avec l'émergence des technologies numériques, ces fondamentaux de l'État se sont transformés avec les technologies numériques. En effet, avec les technologies de Cloud Computing et de Big data, nous constatons que :

- Considérer un État comme un espace géographique délimitée est remis en cause suite à la disparition des frontières entre États avec le Cloud et Internet ;

- Le rapport d'obéissance à l'autorité de l'État n'est plus garanti comme il en témoigne les différences juridiques entre les différents pays. En effet, les plateformes Cloud Computing sont soumises au droit et aux règles juridiques de l'État qui les hébergent et non à celui où se trouvent les utilisateurs internautes.

- L'absence de ce rapport d'obéissance à l'autorité de l'État et sa situation changeante selon chaque plateforme montre bien qu'il n'est plus permanent et durable ;

- L'État n'a plus le monopole de légitimité comme en témoigne la perte de sa souveraineté à l'ère de Cloud Computing. Ainsi, le contrôle de son territoire est remis en cause par la diffusion des technologies numériques.

---

[1] M. WEBER, Economie et Société, Pocket, 2003.

C'est à partir de ces éléments que nous constatons que la conception wébérienne de l'État est remise en cause à travers l'utilisation et la diffusion massive des technologies numériques et nous permet de poser cette définition en tant qu'idéal-type base d'une réflexion sur l'État et ses transformations « techno-logiques ». Nous assistons donc à l'émergence d'un nouveau concept de l'État à savoir : le Cyber-État. Nous y reviendrons en détail dans *la section 1*.

b) Quels rapports de pouvoir à l'ère du Cloud Computing et du Big data ?

Tout ordre sociohistorique est fondé sur des rapports de pouvoir. Un pouvoir « légal-rationnel» qui caractérise un État et passe entre autres par l'adoption de règles de gestion de la société où le sujet se discipline lui-même. Cependant, les avis divergent quant à savoir si nous sommes dans une société disciplinaire ou de contrôle.

Pour Max Weber, toute socialisation passe par une forme de domination, d'adhésion proche de la soumission volontaire qui dépend des qualités que le dominé prête à celui qui commande. L'État, en tant qu'organisation sociale, n'échappe pas à cette règle. Sa légalité est fondée sur la conviction qu'ont les citoyens qu'il est juste de lui obéir.

En effet, lorsque nous aborderons la notion d'obéissance et de la discipline, deux questions se posent :

1. Peut-on encore parler de discipline – des citoyens soit-elle- lorsque cet ordre, pour reprendre l'expression de Claude Lefort[(1)], ne fait plus l'épreuve de son institution. Lefort souhaite souligner par-là que l'ordre n'est plus représenté comme politique ou idéologique.
2. Peut-on parler de la discipline quand le béhaviorisme cybernétique[(2)], œuvre à transformer une adhésion d'ordre éthique à une adhésion « moins éthique ».

Hartmut Rosa[(3)] signale que les sociétés modernes sont régulées, coordonnées et dominées par un régime temporel rigoureux et strict qui n'est pas articulé en termes éthiques. Les sujets modernes peuvent donc être décrits comme n'étant restreints qu'à minima par des règles et des sanctions éthiques, et par conséquent comme étant libres, alors qu'ils sont régentés, dominés et réprimés par un régime-temps en grande partie invisible, dépolitisé, indiscuté sous-théorisé et inarticulé.

---

(1) C. LEFORT, Essais sur le politique. XIXe-XXe siècles, Le Seuil, Paris, 1986.

(2) P. EDWARDS, The Closed World. Cambridge, MIT Press, 1996.

(3) H. ROSA, Aliénation et accélération. Vers une théorie critique de la modernité tardive, La Découverte, 2012.

En tant qu'outils techniques, le Cloud et le Big data se déploient comme dynamiques de surveillance et de contrôle. Cette surveillance, se voit de la sorte ainsi banalisée, puisqu'elle est perçue comme un moyen d'assurer l'intégrité et la sécurité des citoyens. Ainsi, avec le Cloud et le Big data, nous sommes passés du contrôle de la production à la production du contrôle.

La technologie numérique, comme le souligne Mondoux[(1)], est une forme de mémoire porteuse d'une forme de rationalité militaire fondée sur les valeurs de contrôle, de production et de surveillance[(2)].

c) Quel rôle pour les partis politiques dans la transformation numérique ?

Weber[(3)] considère un parti politique comme «*une association reposant sur un engagement formellement libre ayant pour but de procurer à son chef le pouvoir et à ses militants actifs des chances de poursuivre certains objectifs, d'obtenir des avantages personnels, ou de réaliser les deux ensemble* ».

Ainsi, pour identifier un parti politique de d'autres mouvements politiques, Joseph La Palombara et Myron Weiner[(4)] ont élaboré 4 critères qui permettent de distinguer les partis politiques :

- Les partis politiques sont dotés d'une organisation durable. Ils doivent vivre plus que leurs dirigeants ;
- Les partis politiques sont des organisations implantées localement et qui entretiennent des rapports avec d'autres représentations nationales ;
- Les partis politiques expriment leurs volontés explicites d'exercer le pouvoir ;
- Les partis politiques cherchent le soutien populaire à travers 'engagement de ses militants et le soutien électoral.

Nous pouvons donc résumer ces caractéristiques permettant d'identifier un parti politique comme une organisation durable implantée sur le territoire local dans le but d'accéder au pouvoir politique grâce à un soutien populaire.

A travers notre découverte du terrain de recherche en France et au Maroc et suite à nos différents échanges avec ~~les~~ différents acteurs politiques français (Les Républicains, le Parti Socialiste et Union des Démocrates et Indépendants) et marocains (le Parti Socialiste, socialiste, Les Indépendants et le Parti Justice et Développement), nous avons remarqué que les partis politiques n'échappent pas à cette transformation numérique.

---

(1) A. MONDOUX, « Identité numérique et surveillance », Les cahiers du numérique, no 1, pp.1-13, 2011.

(2) A. MATTELART, Histoire de la société de l'information, Paris : La Découverte, 2001.

(3) M. WEBER, Le Savant et le Politique, La Découverte, 2003.

(4) J. LA PALOMBARA et M. WEINER, Political Parties and Political Development, Sociologie Politique, Montchrestien, Paris, 1988.

En effet, ces partis politiques se servent des outils numériques (réseaux sociaux dans le Cloud, traitement de données par le Big data) afin d'afficher leurs programmes et promouvoir leurs campagnes. Ces acteurs politiques essayent de reproduire l'expérience de l'élection du président américain Barack Obama en 2008 (ou ce que l'on appelait Obama 2.0 pour faire référence à l'ère numérique). En effet, Obama avait réussi à mettre ces outils au succès de sa compagne. Cette dernière se jouait également sur près de 15 réseaux sociaux : Myspace, Facebook, Tumblr et même BlackPanet (communauté noire) ou Eons (Babyboomers). Tous des outils dans le Cloud. Barak Obama a également injecté 3,5 millions de dollars dans Google Search pour des besoins de référencement sur Internet.

A partir de ces éléments, nous constatons que la présence sur Internet des partis politiques et leurs représentants ainsi que l'utilisation des moyens numériques pour des fins électorales ne font que transformer la façon dont ces partis politiques cherchent à accéder au pouvoir et être en campagne permanente tout en étant connecté au citoyen par plusieurs outils numériques.

Si nous reprenons donc les quarte caractéristiques données par La Palombara et Weiner[(1)], nous remarquons que:

- Les partis politiques ont une présence durable sur Internet à travers leurs sites web, leurs différents profils sur les réseaux sociaux, l'interaction avec leurs militants, *etc* ;
- Ils sont présents dans tous les territoires à travers les outils numériques. Cet aspect d'être présent sans se déplacer est un aspect fondamental de Cloud Computing ;
- Ils mobilisent leurs militants à travers Internet afin d'exercer le pouvoir. Ils sont en compagne électorale continue et permanente ;
- Ils trouvent des militants et du soutien populaire à travers des plateformes de récoltes des fonds (crowdfunding)[(2)], de sensibilisation à l'attention des militants.

[(1)] J. LA PALOMBARA ET M. WEINER, Political Parties and Political Development, Montchrestien, 1988

[(2)] Le financement participatif (en anglais *crowdfunding*) est une expression décrivant tous les outils et méthodes de transactions financières qui font appel à un grand nombre de personnes pour financer un projet à travers un appel via des plateformes dédiés et disponibles sur Internet.

d) Quelle cybergéopolitique à l'ère de Cloud Computing et de Big data ?

Les 23 et 24 avril 2014, le Grand Hyatt Hotel de São Paulo recevait le Netmundial, autrement dit le Sommet international sur la gouvernance de l'Internet. Les enjeux de cette rencontre internationale sont multiples. Ils sont de l'ordre économiques mais également d'ordre géopolitique comme le soulève Loïc Damilaville, Directeur général adjoint de l'Association Française pour le Nommage Internet en Coopération (AFNIC) : *« L'enjeu majeur d'aujourd'hui pour la gouvernance d'Internet est de savoir si l'on veut que le réseaux des réseaux soit utilisé comme un instrument exceptionnel de partage des connaissances, ou comme une arme géopolitique détenue par une superpuissance qui n'envisage guère d'en partager le contrôle, se réservant le droit de maintenir et de renvoyer ses adversaires, dans l'âge pré-Internet, c'est-à-dire la préhistoire de la société de l'information* ».[(1)]

Les conclusions sont mitigées. D'un côté, les États-Unis ne semblent pas être prêts à réduire leur contrôle sur l'ensemble des instances gérants l'architecture d'Internet aujourd'hui, d'un autre côté, des pays comme la Russie, l'Iran, La Chine, ou Arabie Saoudite souhaitent placer ces instances de gouvernance sous le contrôle de IUT (International Telecommunication Union) avec une implication de l'ensemble des États. Les européens, quant à eux, ont adopté une position modérée plus proche de celle des États-Unis mais souhaitent, cependant, revoir les dispositifs actuels et réduire la domination américaine.

A cela s'ajoute les révélations de Snowden qui ont suscités des réactions diverses à travers le monde. Plusieurs questions se posent sur les origines de cette affaire mais également quels étaient les objectifs recherchés par ces programmes de la NSA ? Qu'est-ce qui a permis une telle expansion ?

Répondre à ses questions n'est pas une chose facile à entreprendre. Cependant, cette affaire a bouleversé les rapports géopolitiques et précisément sur le cyberspace en remettant en cause toute la gouvernance actuelle d'Internet.

L'affaire Snowden n'est pas une simple affaire de renseignement ou une affaire seulement politique, elle a eu des conséquences géopolitiques évidentes au niveau mondial mais également en France. Elle nous rappelle un vieux clivage géopolitique pendant la guerre d'Irak en 2003. En effet, d'un côté, les États-Unis et la Grande-Bretagne et de l'autre, la France et l'Allemagne avec un reste de monde neutre.

Cependant, cette fois-ci, les pays des BRICS sont montés au créneau et ont manifesté un mécontentement à l'égard des pratiques des États-Unis. Pour cause, les pays des BRICS ne n'acceptent plus la prédomination américaine.

[(1)] Cité par FAYON David dans Géopolitique de l'Internet, Paris, Economia, 2013, p. 1.

Par exemple, suite à cette affaire, le Brésil s'est rapproché de l'Argentine malgré les différences séculaires entre les deux pays. L'objectif est de mieux se protéger suite aux révélations d'écoutes de la présidente brésilienne[(1)]. Suite à ces révélations, probablement l'ensemble des pays partout dans le monde ont pris chacun des dispositions pour augmenter leur propre protection et assurer une autonomie numérique.

L'affaire Snowden a eu des conséquences géopolitiques mais sans actions concrètes à l'encontre des États-Unis. En effet, dans ce contexte numérique dominé par des solutions en majorité nord-américaines, il est encore difficile d'être indépendant des États-Unis dans la gestion de son propre cyberspace. En effet, la théorie de Joseph Nye décrit une puissance douce « soft power »[(2)] qui viendrait soutenir la puissance traditionnelle. La NSA, à travers ses programmes de surveillance, a démontré qu'elle a une puissance traditionnelle mais dans un nouveau espace : Internet.

Depuis que l'économie mondiale s'est configurée autour des technologies du Cloud et du Big Data, les frontières géographiques entres États se sont disparues, les échanges commerciaux et de données à travers les plateformes Cloud Compuitng échappent de plus en plus au contrôles des États souverains.

Les données des utilisateurs sont traitées par des technologies Big data et permettent de surveiller en masse et de contrôler le comportement de ces personnes loin des jurisprudences nationales. Ainsi, l'Internet est devenu un espace de conflit géopolitique où les questions de souveraineté et du respect de la vie privée sont devenues cruciales. Alors qu'en même temps et malgré ses origines militaires, les tentatives de plier l'Internet, par des moyens techniques et réglementaires, au respect des frontières nationales n'ont pas abouties. C'est dans ce contexte qu'une gouvernance de l'Internet élargie à l'échelle planétaire se positionne comme alternative pour assurer le bon fonctionnement du « réseau des réseaux » et apaiser les différentes tensions afin de garantir le bon usage d'Internet dans l'avenir.

---

(1) O. KEMPF, Introduction à la cyber stratégie, Economica, 2015.

(2) Le concept de *soft power* désigne les méthodes d'influence développées par un Etat qui ne s'appuient pas sur la violence mais sur des éléments idéologiques ou culturels en vue de satisfaire les intérêts de la nation qui les met en œuvre. Le soft power s'exerce sous des formes de coercition, d'incitation, de séduction ou encore d'influence sur le choix des problèmes politiques apparaissant comme prioritaires, avec comme impératifs la crédibilité et la légitimité. Le terme de soft power fut pensé et décrit par Joseph S. Nye dans son ouvrage paru en 1990, Bound to Lead, Basic Books, U.S.A, 1991.

10. Annonce du plan

Ce travail s'organise autour d'une *introduction,* 3 parties*, une conclusion, une bibliographie et une partie comprenant des annexes.*

L'introduction :

Elle est composée de 10 points principaux qui fixent le cadre de la recherche, expose la méthodologie suivie ainsi que l'ensemble des théories mobilisées. Nous avons également essayé de montrer l'importance de traiter ce sujet et nous avons expliqué nos différents choix et motivations. Par la suite, nous avons présenté la question de recherche d'une façon générale et nous l'avons détaillée en questions spécifiques pour mieux appréhender les différents points qui seront couverts par ce travail.

Partie 1 : Comprendre l'action publique à l'ère du Cyber-État

Chapitre 1 :

Le chapitre est une étude de cas réalisée que nous avons réalisé conjointement avec des des partenaires situés aux Etats-Unis et qui étaient intéressés par savoir comment l'administration publique française réagit aux transformations numérique. Ces deux partenaires sont:

- *Engaged Public* est un organise de conseil en stratégie et spécialisé dans les politiques publiques et travaille principalement pour l'Etat de Colorado.
- *CausesLabs* est une association qui travaille sur des projets humanitaires à travers le développement des outils numériques pour avoir un impact positif dans le quotidien des citoyens.

L'objectif de cette étude de cas est d'adapter un outil, appelé « *Balancing Act »*, de contrôle de budget des collectivités territoriales au contexte français et plus précisément pour la commune de Boulogne-Billancourt. Cet outil qui sera ouvert directement aux citoyens a pour objectif de donner la main aux citoyens pour contrôler la gestion du budget de leur ville et de contrôler le travail des élus locaux. C'est une solution qui combine à la fois l'ensemble les différentes technologies étudiées dans ce travail de recherche. En effet :

- Elle est disponible dans le Cloud ;
- Elle se base sur des technologies Big data ;

L'objectif principal est de montrer l'impact du numérique sur le fonctionnement d'une institution publique – collectivité territoriale. Cette étude alimente les différentes notions qui seront développées par la suite dans les prochains chapitres.

Chapitre 2

Nous avons essayé à travers ce chapitre d'étudier l'action publique afin d'en comprendre le fonctionnement sous le spectre numérique. Nous avons essayé également de comprendre

l'historique de la construction de l'État, ses origines puis de clarifier les différentes notions liées à l'État comme le secteur public, le service public et la fonction publique ainsi que lever toutes les nuances liées à ces concepts dans le contexte français et marocain.

Par la suite, nous avons essayé d'étudier la notion de l'État selon la définition donnée par Weber et de comprendre si cette définition est toujours valable avec l'ensemble de transformation numérique à l'ère de Cloud et de Big data et voir si une nouvelle conception pourrait en émerger à savoir : le Cyber-État

Chapitre 3 :

Dans ce chapitre, nous allons essayer de comprendre le champ des politiques publiques et particulièrement celui des cyber-politiques publiques.

Dans un premier temps, nous essayons de donner une définition d'une politique publique puis à d'introduire un nouveau terme celui de la cyber-politique publique. Nous présenterons par la suite la notion de l'analyse des cyber-politiques publiques et en quoi consiste une telle analyse.

Nous détaillerons par la suite l'approche séquentielle qui permet une analyse de bout en bout d'une cyber-politique publique. Ensuite, nous aborderons les limites de cette approche séquentielle.

Nous verrons également le rôle des acteurs et des groupes d'intérêts dans le cadre d'élaboration des cyber-politiques publiques en France et au Maroc.

Par la suite, nous verrons le phénomène « *d'uberisation* » des politiques publiques et comment l'État fait face aux nouveaux problèmes d'un nouveau type provoqué par le numérique.

Pour conclure cette section, nous tenterons de comprendre la démarche d'une cyber-politique publique à travers une étude de cas avec la plateforme Cloud Computing « Uber » pour les taxis. Nous expliquerons les différentes notions étudiés dans ce chapitre à partir du cas de l'arrivée de la plateforme « Uber » en France et au Maroc : Émergence du problème, inscription sur Agenda politique, réponse politique, etc.

Partie 2 : La société numérique à l'ère du Cyber-État

Chapitre 1 :

Dans ce chapitre nous avons essayé de comprendre l'évolution numérique du comportement social des individus. En effet, ce dernier a évolué en parallèle de l'évolution de la technologie en multipliant les formes d'interaction. Ainsi, à travers ce chapitre, nous verrons:

- La vie en ligne à l'ère de Cyber-État : Nous essayerons de comprendre la contribution volontaire du citoyen au développement des savoirs et connaissances partagées. Ainsi, comprendre les motivations des individus pour contribuer à la construction d'une connaissance partagée à travers un ensemble de communautés organisées en ligne ;
- L'identité numérique ou la cyber-Identité: Comprendre cette expression de soi à travers des blogs, des statuts, …, visant à développer une sociabilité en ligne ;
- Les problématiques du traitement des données personnelles ainsi que toute la législation associée ;
- Nous analyserons les contributions de plusieurs institutions dans ce débat lié à la vie social en ligne : CNIL, CNDP, G29, Chaire « Valeurs et politiques des informations» et la « Quadrature du Net ».

Chapitre 2 **:**

Dans un contexte de lutte contre le terrorisme sous toutes ses formes, le débat politique français et marocain est agité par une inquiétude grandissante autour du déploiement de dispositifs numériques de surveillance généralisée par l'adoption de plusieurs dispositifs de lois (loi anti-terrorisme, loi relative au renseignement, …).

Ainsi à travers cette section, nous allons découvrir la notion de cyberspace où se déploie les enjeux politiques du numérique, des intérêts économiques et stratégiques qui promeuvent les méthodes de surveillance. Nous y aborderons également les notions de la cybermenace et de la cybersurveillance ainsi que la notion de la cybersouveraineté et comment l'État ou le Cyber-État peut ré affirmer son droit à l'ère de la sécurité nationale.

Chapitre 3

A travers ce chapitre, nous essayons d'étudier les effets de la géopolitique d'Internet et la cybergéopolitique sur le fonctionnement du Cyber-État et les relations internationales.
Cette section traite les points principaux :

- *Gouvernance d'Internet* : A travers cette partie, nous essayons de définir le concept de la gouvernance et son application sur Internet. Nous évoquerons les enjeux associés à la mise en place d'une gouvernance d'Internet à l'échelle mondiale afin de préserver son avenir. Nous analyserons également la mise en place des institutions internationales en charge d'assurer cette gouvernance ;
- *Instances mondiales ou « la république des ingénieurs »*: A travers cette partie, nous analyserons l'ensemble des institutions qui opèrent pour une gouvernance d'Internet et qui permettent d'assurer son développement dans les bonnes conditions. Nous expliquerons également les procédures d'évolution des protocoles et la gestion de l'infrastructure technique Internet dans son sens large ;
- *Les rapports du pouvoir dans la gouvernance Internet* : nous essayons ici de présenter les enjeux futurs de l'internet d'aujourd'hui. Entre la concurrence des plateformes,

l'investissement dans les infrastructures, la gestion des instances de gouvernance, le partage des bénéfices, la taxation des activités, *etc*. Tous ces paramètres risquent de remettre en cause à tout moment le fonctionnement actuel d'Internet ;

- *Concept de neutralité du Net* : nous présenterons dans cette partie le concept de la neutralité du Net. Nous essayerons de donner des définitions précises, d'analyser les enjeux et les motivations associés ainsi que le rôle des pouvoirs publics dans l'encadrement des activités liées à Internet ;

Partie 3 : Fondements techniques du Cyber-État

Chapitre 1 :

L'objectif de ce chapitre est de comprendre, techniquement et fonctionnellement, l'ensemble des technologies étudiées dans le cadre de notre travail de recherche. Ainsi, il s'agit de comprendre le fonctionnement de l'Internet, du Cloud Computing. Nous essayerons d'expliquer le lien entre ces technologies ainsi que les évolutions possibles. Cette section se décompose en deux parties principales :

- Première partie est dédiée à une présentation de l'Internet et son rôle dans la transformation numérique en cours. Nous y présenterons également l'apport de l'Internet dans le développement des technologies étudiées : Le Cloud Computing et le Big data. Les thèmes de cette partie sont donc :
  - Le développement de l'Internet ;
  - Le rôle de l'Internet dans le fonctionnement du Cyber-État.
- Deuxième partie est dédiée au Cloud Computing. Dans cette partie nous présenterons une revue de littérature de Cloud Computing et ses différentes définitions et ses architectures et modèles de déploiement. Nous essayerons de clarifier les différentes notions liées au Cloud Computing et nous finirons par une présentation des plans Cloud français et marocain ainsi que la notion du cloud souverain. Dans cette partie, nous traiterons donc :
  - Le Cloud comme fondement technique du Cyber-État ;
  - Le Cloud souverain à l'ère de Cyber-État ;
  - Vers des référentiels de confiance à l'ère de Cloud
  - Le plan Cloud dans le cadre de la nouvelle France industrielle
  - Quel Cloud pour le Cyber-État marocain ?

Chapitre 2:

L'objectif de cette section est de proposer une approche technique et fonctionnelle de la technologie du Big data. .

En effet, à travers cette section, nous présenterons l'ensemble des définitions de ce terme et ses différentes caractéristiques. Nous présenterons le métier de « *data scientist* » ainsi que son rôle dans le secteur public. Nous terminerons par une présentation des outils utilisés par les technologies Big data ainsi que les différentes initiatives de l'État français et marocain en matière de Big data.

Les thèmes principaux traités sont :

- Présentation de la technologie de Big data ;
- La fonction de « *Chief Data Office* » dans le cyber-secteur public ;
- Les outils du Big data ;
- Le plan Big data (Nouvelle France industrielle) ;
- La mission Etalab (Opendata).

Chapitre 3 :

Ce dernier chapitre permet de montrer que le Cloud et le Big Data ne sont les seules technologies pour un Cyber-Etat d'avenir. Dans ce domaine en perpétuel évolution, les technologies changent rapidement et leurs impacts également. L'Etat, ou le Cyber-Etat, doit être en mesure de suivre cette évolution dans la quantité et dans la qualité. L'avenir annonce beaucoup d'autres technologies de rupture qui changeront nos modes de vie et aussi transformerons le fonctionnement de l'État vers le Cyber-État.

Bibliographie :

Notre revue bibliographique tente de couvrir l'ensemble des aspects abordé dans ce travail de recherche. En effet, les notions traitées dans nos recherches touchent à plusieurs domaines. Par conséquent, c'est un travail pluridisciplinaire. Cependant, il s'inscrit dans le domaine de la science politique et plus précisément dans le domaine des politiques publiques.

Pour réaliser ces travaux, nous nous sommes appuyés sur plusieurs références de base, à savoir :

- *Références de science politique* : En effet, nous avons pu comprendre la notion de l'Etat et de la politique publique entre autre. Nous avons pu donc nous appuyé sur des auteurs de références comme Weber, Foucault, Lasswell, Wiener.

- *Références en sciences de gestion* : Comme nous l'avons signalé précédemment, il nous semble intéressant que les sciences de gestion abordent ces questions de Cloud Computing et de Big data en donnant un discours de légitimation à ces systèmes. Cependant, Il faut considérer ces références d'un point de vue critique vu que la grande partie de leurs discours apparaissent comme légitimateur de pouvoir dans ce champ comme le souligne Bourdieu. Aussi, nous retrouvons dans ces références de

sciences de gestion du sens commun considéré comme non critique à l'étude de notre objet de recherche.

- *Références techniques* : Pour comprendre le Cloud Computing et le Big data, nous avons utilisé des références techniques qui nous ont permis d comprendre techniquement et fonctionnellement le fonctionnement de telles technologies. Nous avons pu comprendre ces notions et notre formation de base d'ingénieur nous a permis d'y arriver ;

- *Rapport et études diverses* : Nous nous sommes appuyés sur des rapports et des études publiés par des institutions internationales et des grands cabinets de conseil (banque mondial, OCDE, McKinsey, BCG, *etc*) afin de comprendre les différents impactes des technologies étudiées sur la société, l'économie et les politiques publiques. Ces différentes études nous ont permis également d'aborder certaines propositions et transformations à venir liées à l'usage des cyber-technologies.

La liste complète de notre bibliographie est organisée dans un ordre alphabétique pour faciliter la recherche et l'identification des auteurs.

Partie 1

Comprendre l'action publique à l'ère du Cyber-État

I. Partie 1 : Comprendre l'action publique à l'ère du Cyber-État

La sociologie de l'action publique constitue un domaine bien institutionnalisé de la science politique. En effet, la mutation des sciences politiques avec l'ère numérique implique une diversification des approches, des objets de recherche et des perspectives d'analyse de la notion même d'État. Ainsi, Cette diversification se déroule à travers l'intervention des acteurs publics dans les réformes de modernisation de l'action publique et de l'ensemble des administrations de l'État.

Nous proposons donc à travers cette première partie d'étudier la notion de l'État afin d'en comprendre le fonctionnement et l'historique.

Par la suite, nous ferons une analyse de l'État à l'ère du Cloud Computing et du Big data à partir de la définition qu'en donne Max Weber (de l'État). Nous essayerons de comprendre si cette définition idéal-typique proposée par Weber est toujours adaptée avec la transformation numérique de la société ou si, au contraire, des nouvelles définitions doivent être apportées pour s'adapter aux nouvelles exigences voire à l'émergence d'un nouveau concept : le Cyber-État.

Nous essayons également de comprendre l'historique de sa construction puis de clarifier les différentes limites entre le secteur public, le service public et la fonction publique. L'objectif est de lever toutes les nuances liées à la compréhension de l'ensemble de ces concepts voire si l'ensemble de ces notions sont transposables pour un « Cyber-État » : « cyber-secteur public », « cyber-service-public », … . Nous aborderons également le sort de la fonction publique à l'ère du Cyber-État et comment la fonction publique devrait évoluer avec les technologies numériques.

Nous présenterons par la suite la notion de la performance des activités de l'État et nous conclurons avec les différentes initiatives de modernisation en France et au Maroc. L'objectif est de comprendre le processus de modernisation de l'État à travers la mise en place des politiques publiques de modernisation et plus particulièrement modernisation numérique.

1. Chapitre 1 : Étude de cas : Le Cloud Computing et le Big data au service de l'action locale

A. Introduction

a) Contexte

Nous souhaitons à travers cette étude de cas de montrer l'apport concret de la technologie et précisément du Cloud Computing dans la diffusion d'une démocratie locale en développant un outil technologique qui permet aux citoyens de suivre, contrôler, faire des recommandations sur la gestion de leur localité.

En effet, nous pensons que notre expertise technique acquise pendant la formation initiale d'ingénieur et durant des années passées au sein du monde professionnel combinée avec la connaissance du secteur public que nous avons étudié pendant ces années de recherche va nous permettre de mettre en place un tel outil technologique d'un point de vue technique mais également fonctionnel.

Cette étude de cas a été donc réalisée pendant 6 mois en collaboration avec des partenaires américains et vise principalement à comprendre :

- Le fonctionnement d'une collectivité locale ;
- Le développement d'un outil dans le Cloud ;
- Mesurer l'impact d'une telle initiative ;
- Evaluer l'adoption de cet outil par la collectivité et par le citoyen.

Dans la suite de cette étude, nous allons expliquer le fonctionnement d'une collectivité locale, la gestion de son budget puis nous expliquerons la méthodologie suivie pendant cette étude et nous allons conclure avec une description des travaux réalisés ainsi qu'une conclusion générale en détaillant les résultats obtenus.

b) Qu'est-ce qu'une collectivité territoriale ?

Les collectivités territoriales sont des personnes morales de droit public distinctes de l'État et bénéficient à ce titre d'une autonomie juridique et patrimoniale. L'article 72 de la Constitution française de 1958 prévoit leur existence. Cet article assure aux collectivités une libre administration par des conseils élus. Elles disposent ainsi d'une autonomie juridique et patrimoniale mais ne disposent que de compétences administratives attribuées par la loi.

> **[Article 72]**
> *« Les collectivités territoriales de la République sont les communes, les départements, les régions, les collectivités à statut particulier et les collectivités d'outre-mer régies par l'article 74. Toute autre collectivité territoriale est créée par la loi, le cas échéant en lieu et place d'une ou de plusieurs collectivités mentionnées au présent alinéa.*
>
> *Les collectivités territoriales ont vocation à prendre les décisions pour l'ensemble des compétences qui peuvent le mieux être mises en œuvre à leur échelon.*
>
> *Dans les conditions prévues par la loi, ces collectivités s'administrent librement par des conseils élus et disposent d'un pouvoir réglementaire pour l'exercice de leurs compétences.*
>
> *Dans les conditions prévues par la loi organique, et sauf lorsque sont en cause les conditions essentielles d'exercice d'une liberté publique ou d'un droit constitutionnellement garanti, les collectivités territoriales ou leurs groupements peuvent, lorsque, selon le cas, la loi ou le règlement l'a prévu, déroger, à titre expérimental et pour un objet et une durée limités, aux dispositions législatives ou réglementaires qui régissent l'exercice de leurs compétences.*
>
> *Aucune collectivité territoriale ne peut exercer une tutelle sur une autre. Cependant, lorsque l'exercice d'une compétence nécessite le concours de plusieurs collectivités territoriales, la loi peut autoriser l'une d'entre elles ou un de leurs groupements à organiser les modalités de leur action commune.*
>
> *Dans les collectivités territoriales de la République, le représentant de l'État, représentant de chacun des membres du Gouvernement, a la charge des intérêts nationaux, du contrôle administratif et du respect des lois. »*

c) Les réformes des collectivités

Les collectivités territoriales françaises ont subi une série de réformes dans le cadre de la décentralisation[(1)]. Cependant, comme le souligne Jean-Claude Thoenig[(2)], même si elle concerne au premier chef les collectivités locales, la politique de décentralisation peut aussi s'analyser comme une politique publique impulsée et conduite par le sommet de l'État, ainsi, il précise que « *en matière de décentralisation, le pouvoir politique gouverne de façon centralisée* ». Ainsi, la décentralisation a été concrétisée par l'adoption des réformes suivantes :

- En 1982-1983, les lois Defferre[(3)] créent les régions et mettent fin au contrôle à priori des préfets sur les décisions des collectivités. Ces lois constituent ce que l'on appellera par la suite l'Acte I de la décentralisation.
- En 2003-2004, l'Acte II de la décentralisation transfère certaines compétences de l'État vers les régions et départements ;
- En 2008-2012, des réformes visent à supprimer la clause de compétence générale et à changer le mode de scrutin des conseils généraux et régionaux ;
- depuis 2012, l'Acte III de la décentralisation revient en partie sur la précédente réforme et vise à modifier les modes de scrutin, réduire le nombre de régions et leur transférer plus de compétences.

Cependant, il n'y'a pas de bonne décentralisation sans une déconcentration[(4)] parallèle des services de l'État. Les élus locaux, dotés de nouvelles compétences, doivent pouvoir s'adresser au niveau local à un représentant de l'État dont les attributions lui permettent d'engager l'État sans en référer systématiquement à l'échelon central.

Ainsi, un des objectifs poursuivis par la politique de décentralisation et déconcentration est de rapprocher le processus de décision des citoyens et de favoriser ainsi l'émergence d'une véritable démocratie de proximité qui est au cœur de notre étude du cas.

---

(1) La décentralisation en France est un processus d'aménagement de l'État unitaire qui consiste à transférer des compétences administratives de l'État vers des entités (ou des collectivités) locales distinctes de lui. Avec le transfert de certaines compétences à une collectivité, l'État doit aussi transférer les ressources correspondantes. Cette décentralisation de la République est inscrite dans la Constitution dont l'article 1 précise «*l'organisation [de la République française] est décentralisée* » (définition tirée du www.vie-publique.fr Qu'est-ce que la décentralisation).

(2) J-C THOENIG et Y. MENY, Politiques publiques, PUF, 1989.

(3) Les « lois Defferre » (du nom de l'ancien ministre de l'Intérieur et de la Décentralisation), adopté en en 1982, correspondent à la volonté politique de la gauche, arrivée au pouvoir en 1981, de réaliser une profonde décentralisation de l'administration française.

(4) La déconcentration est un processus d'aménagement de l'État unitaire qui consiste à implanter dans des circonscriptions locales administratives des autorités administratives représentant l'État. Ces autorités sont dépourvues de toute autonomie et de la personnalité morale. Aujourd'hui, sont des autorités déconcentrées : les préfets (départements, régions), les recteurs (académies), les maires (communes), etc.

B. Gestion du budget des collectivités

a) Contexte

La décentralisation et l'élargissement des compétences des collectivités, et surtout la libéralisation de leur financement, nécessitent de mettre à la disposition des élus, des citoyens et des partenaires financiers des collectivités des informations et des indicateurs fiables et précis sur leur situation financière et sur l'impact financier de l'action publique. Ainsi, la comptabilité des collectivités repose sur une démarche a posteriori puisqu'il s'agit de retracer les mouvements financiers exécutés. Elle est tenue par un ordonnateur, au moyen de ce qu'on appelle le compte administratif. Le comptable public tient, pour sa part, le compte de gestion. Les deux comptes doivent coïncider.

Ainsi, les collectivités territoriales élaborent plusieurs documents budgétaires avant et pendant l'exercice. À l'issue de la gestion, le compte administratif qui arrête le résultat de l'exercice doit être voté. Même si leur portée juridique est très différente, budget et comptabilité portent sur les mêmes objets, et doivent donc rendre compte des masses financières selon les mêmes grilles d'analyse, les mêmes nomenclatures.

La gestion budgétaire de la collectivité cherche notamment à améliorer l'information budgétaire et financière permettant de reclasser les recettes et les dépenses selon les politiques conduites par la commune (enseignement, culture, action économique, administration générale, *etc*.).

b) Problématique de notre étude : vers une cyberdémocratie locale ?

Les lois « Defferre » et les autres lois de décentralisation transfert des compétences de l'État vers les collectivités locales et réactivent le rôle et le pouvoir de ces dernières. En revanche, des collectivités locales vers la population rien ou presque n'est transféré ce qui va à l'encontre de la démocratie dite « locale ».

En effet, la notion de « démocratie locale » apparaît pour la première fois dans la loi d'orientation du 6 février 1992 pour l'administration territoriale de la République. Ainsi, la loi du 27 février 2002 relative à la démocratie de proximité vise à permettre une meilleure association des citoyens aux décisions locales, en renforçant la démocratie participative et les droits de l'opposition au sein des assemblées délibérantes.

Cependant, l'acceptation de la notion de « démocratie locale » est très restreinte. En effet, elle désigne le droit de la population à l'information et à la consultation. Elle tend à améliorer l'information et la participation des habitants comme la mise à disposition des documents budgétaires.

C'est ainsi que dans la cadre de notre recherche, nous avons pu développer un cas pratique qui permet de mettre à disposition des citoyens un outil technologique, disponible dans le Cloud Computing et utilisant les technologies de Big data, qui va permettre à ces citoyens de

s'informer, de contrôler et de participer à la gestion budgétaire de leurs collectivités. Cette démarche s'inscrit dans la promotion d'une cyberdémocratie locale.

Ainsi, à travers ce cas pratique, et en partenariat avec la mairie de Boulogne-Billancourt dans les Hauts-de-Seine, nous avons pu adapter un outil de contrôle du budget d'une collectivité territoriale au contexte français. Cet outil est déjà utilisé par des municipalités aux Etats-Unis selon des règles américaines locales. Ainsi, nous avons essayé d'évaluer l'adoption des outils technologiques par la population et d'évaluer les degrés d'acceptation de ce type d'outils dans la gestion des affaires locales. Il s'agit d'un travail conduit conjointement par plusieurs partenaires engagés.

c) Acteurs engagés

L'outil que nous avons développé a été le fruit d'une collaboration entre la mairie de Boulogne-Billancourt (France), l'association CausesLabs (États-Unis), Engaged Public (Organisme spécialisé en politique publique aux États-Unis) et nous même ici en France. Les personnes impliquées sont donc :

- Christine Lavarde, adjointe maire, responsable du budget et des finances à la mairie de Boulogne-Billancourt dans la commune des Hauts-De-Seine ;
- Chris Adams, directeur général d'Engaged Public, basé à Denver aux États-Unis ;
- Brenda Morrison, associée Engaged Public en charge du développement internationale ;
- Kevin Amirehsani: responsable des relations Institutionnelles ;
- Sarah Solano directrice de développement au sein CausesLabs.

Ainsi, Nous avons travaillé sur plusieurs mois avec la ville de Denver aux États-Unis en partenariat avec deux organismes locaux[(1)]:

- *Engaged Public* est un organisme de conseil en politiques publiques à destination du gouvernement américain. Il est situé dans la ville de Denver dans l'État du Colorado, aux États-Unis.
- *CausesLabs* une association qui travaille sur des projets humanitaires avec un impact positif dans la société tout en utilisant les outils technologiques.

---

(1) Nos méthodes de travail et d'échanges avec les partenaires américains étaient sous forme de Conférences téléphoniques par Skype et un échange quotidien par mail. Nous avons également construit un espace collaboratif d'échange de documents produits.

C. Description des travaux

a) Méthodologie du travail :

Afin de répondre à notre problématique, notre démarche consiste à comprendre les architectures techniques et fonctionnelles de la solution « *Balancing Act* », de comprendre le contexte de la gestion des budgets au sein des collectivités françaises et par la suite adapter l'outil « *Balancing Act* » selon les différentes règles de gestion.

Une fois la partie technique et fonctionnelle maitrisée, il nous fallait avoir accès aux données financières de la mairie de Boulogne-Billancourt. En effet, nous avons pu collaborer avec madame Christine Lavarde qui nous a donné accès à des données « non critiques » donc publiques. Nous avons pu donc les intégrer dans le cadre du développement de « Balancing Act » selon les contraintes et les règles françaises. Ainsi, deux types de données sont utilisés :

- Des données factuelles en analysant des documents disponibles sur Internet.
- Des données déclaratives à travers les recueils d'entretiens avec les différents acteurs impliqués dans cette étude.

Une fois les données sont disponibles et préparées, nous avons pu les intégrer dans l'outil « *Balancing Act* » comme nous le montrerons dans la partie résultats des travaux ci-dessous.

b) Les objectifs recherchés

L'outil « *Balancing Act* » est une application informatique déployée dans le Cloud et qui permet de traiter les données publiques en masse via les technologies de Big data. Elle est accessible sur PC, tablette et téléphone mobile.

Cet outil permet donc les fonctionnalités suivantes :

- Le suivi des budgets des collectivités territoriales à temps réel ;
- Rendre la gestion de l'argent public transparent aux citoyens ;
- Augmenter la transparence dans la gestion des budgets des collectivités ;
- Faire adhérer les citoyens au développement des projets locaux ;
- Collecter les données et les retours des citoyens. Ainsi, prioriser les attentes/actions ;
- Cultiver une relation de confiance et de transparence avec les citoyens ;

Ainsi, à travers cet outil, notre objectif est de développer et de ré inventer le mode de fonctionnement de la collectivité de demain tout en nous appuyant sur les technologies de Cloud et de Big data.

c) Description des résultats

Le résultat concret de nos travaux consiste à un prototype de simulation de la gestion du budget qui n'impactent pas les données réelles de la mairie. En effet, l'outil est alimenté par des données fictives qui permettent de stimuler le fonctionnement attendu.

Ainsi, l'outil « *Balancing Act* » n'est intégré ; à ce stade ; au système d'information de la commune. Il s'agit des données que nous avons répliquées pour des besoins de test et simulation. Ainsi, avec ce prototype développé, nous avons pu mettre en place les fonctionnalités de base suivantes :

i. Fonctionnalités à destination de la collectivité:

- Mettre le budget à disposition du citoyen par catégories de dépenses et revenues : En effet, avec cette option, la mairie peut mettre à disposition des citoyens son budget sous deux catégories : Dépenses et Revenues. Chacune des catégories est composée de sous catégories comme le montre la figure suivante issue de l'application développée :

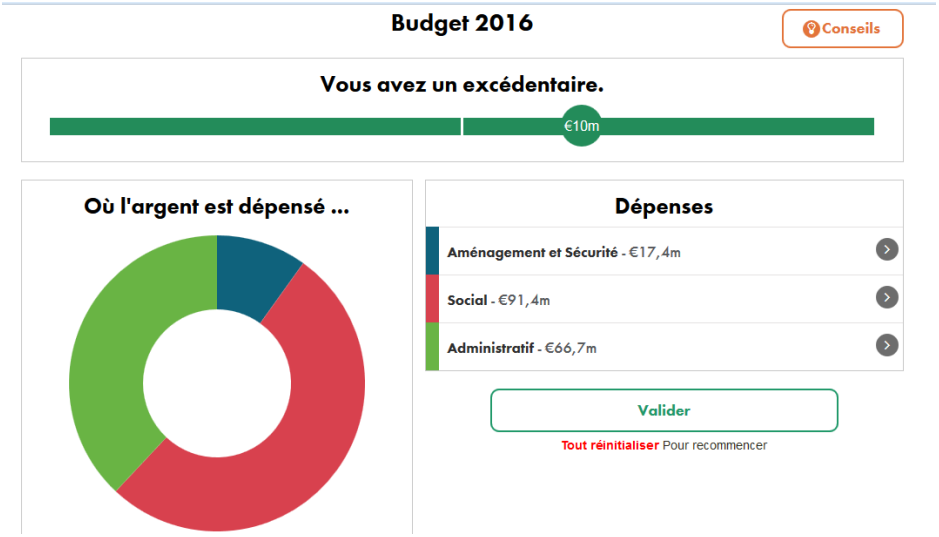


Schéma 01 Gestion de budget à travers de l'application « Balancing Act »

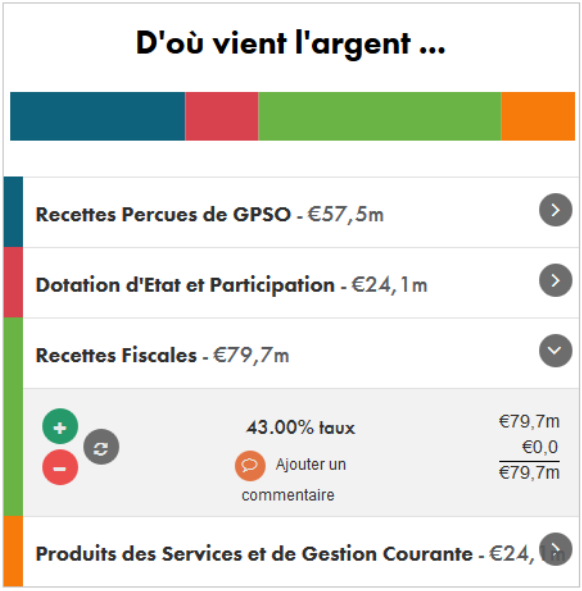


Schéma 02 : Origines des ressources dans l'application « Balancing Act »

- Mise à disposition d'un tableau de bord selon les différents retours citoyens

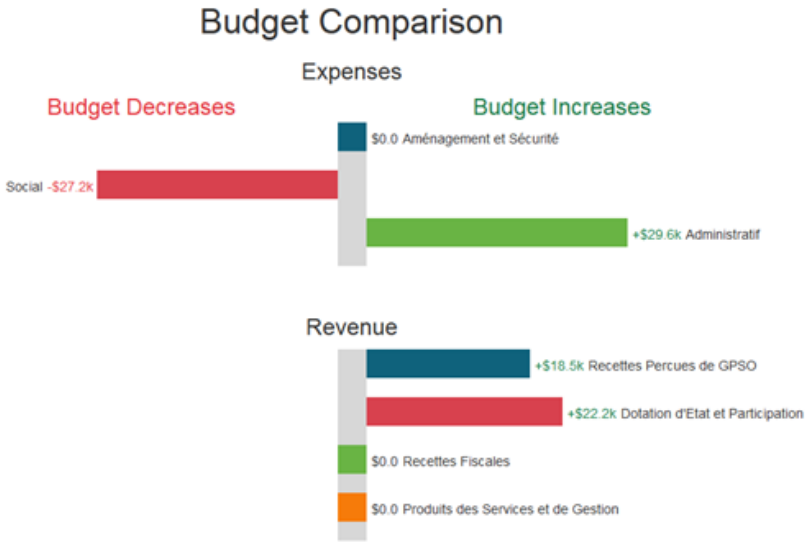


Schéma 03 : Comparaison des budgets dans l'application « Balancing Act »

- Mise à disposition des retours des citoyens avec les différentes informations statistiques pour mieux les connaitre : âge, sexe, etc.
- Envoies des emails / alertes / notifications aux citoyens si un seuil est dépassé pour une catégorie particulière.
- Mise à jour continue du budget et à temps réelle selon les retours citoyens.

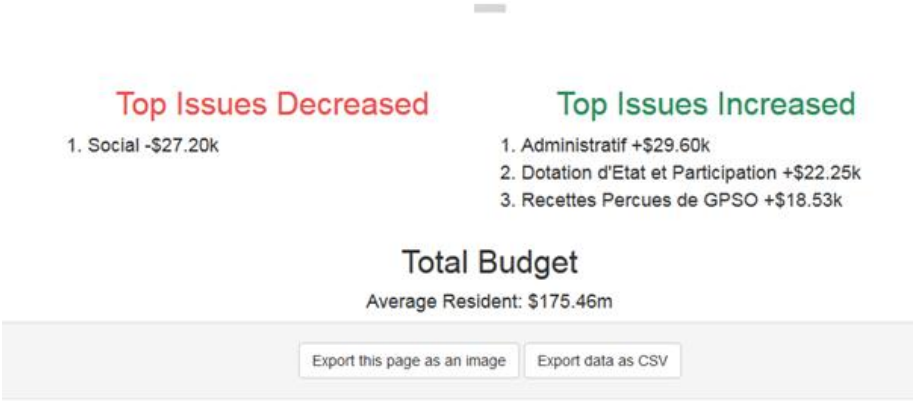


Schéma 04 : Comparaison des budgets dans l'application « Balancing Act »

ii. Fonctionnalités à destination du citoyen :

- Modifier un budget (dépense ou revenue) par le citoyen en rajoutant les montants et les commentaires associés. Cette modification n'impacte pas le projet réel mais permet à la commune d'analyser les avis et les préoccupations des citoyens et ainsi les prendre en considération.

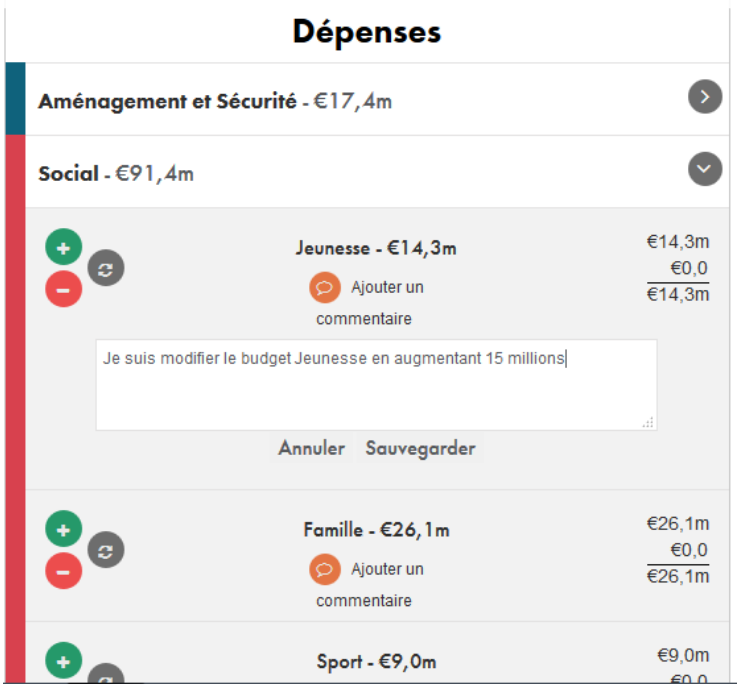


Schéma 05 : Affichage des dépenses dans l'application « Balancing Act »

- Faire proposition à la collectivité avec des commentaires associés
- Emettre des remarques d'ajustement sur les budgets en cours

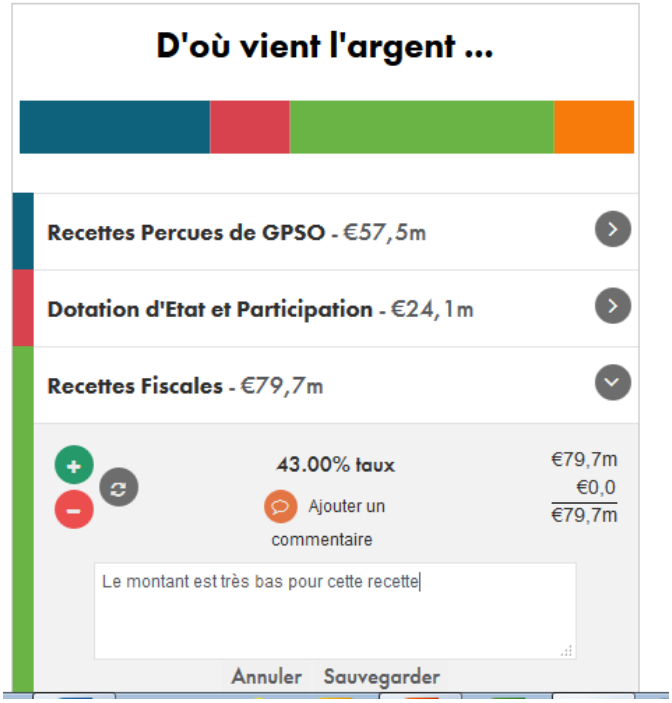


Schéma 06 : Origines des ressources dans l'application « Balancing Act »

- Avoir une vision temps réel sur le budget et son évolution
- Partager ses réflexions avec ses amis sur les réseaux sociaux /mails / sa page personnelle, etc.
- Mettre des alertes par catégories de dépenses /revenues

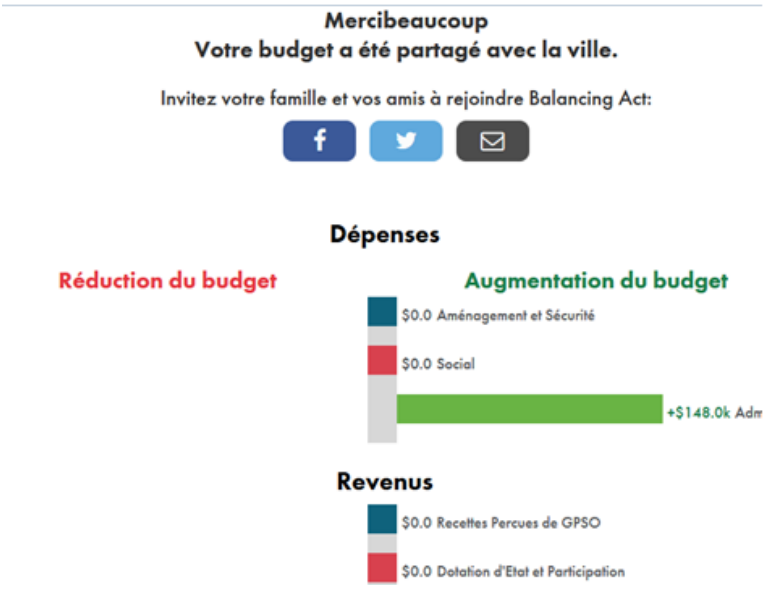


Schéma 07 : Affichage du récapitulatif dans l'application « Balancing Act »

D. Les conclusions de l'étude de cas

Comme nous l'avons décrit précédemment, une démocratie locale permet de transférer certaines compétences de l'État vers des collectivités locales. Cependant, le transfert de certaines de ces compétences par la collectivité elle-même vers le citoyen n'est pas, en tout cas pour le moment, envisageable par les collectivités. Un constat que nous avions remarqué pendant nos différents échanges avec les acteurs locaux à la mairie de Boulogne-Billancourt. En effet, nous avons remarqué une réticence dans l'adoption de l'idée d'ouvrir le débat autour de la gestion des budgets aux citoyens. Ainsi, parmi les arguments avancés par les personnes concernées on trouve :

- La difficulté à simplifie les processus d'adoption pour qu'ils soient compréhensibles au simple citoyen.
- L'ouverture élargie du débat risque de perturber les travaux et donc d'avoir du retard sur la réalisation des projets de la collectivité.
- Une éducation technique et technologique des citoyens à l'utilisation de ces outils doit être prise en compte afin de permettre une telle adoption.

Nous remarquons que ces arguments révèlent une résistance au changement qui pourrait être provoqué par le numérique. Ainsi, le secteur public et précisément les collectivités locales dans notre cas, ne sont pas à l'abri d'une transformation de leur mode de fonctionnement. En effet, les acteurs locaux craignent une « *uberisation* » de leur travail si nous mettons en place de tels outils technologiques. Des outils cependant nécessaires pour diffuser une démocratie locale et faire adhérer les citoyens à la gestion locale ainsi avoir un contrôle sur le travail des élus et par conséquent pouvoir choisir librement pendant les prochaines élections en se basant sur des indicateurs fiables fourni par cet outil «neutre».

A ce stade, l'outil reste un outil de simulation. Ainsi, nous avons eu une réflexion approfondie pour le développer et le proposer à d'autres mairie ainsi permettre une diffusion élargie d'une démocratie locale dont la participation du citoyen est au centre de ses priorités. Nous avons donc identifié les axes principaux suivants à développer dans l'avenir:

- Réadaptation des règles par rapport à la gestion réelle d'une collectivité ;
- Prendre en compte les contraintes terrain de la gestion des budgets ;
- Développement de plusieurs fonctionnalités: interconnexion avec d'autres collectivités, comparaison des résultats, réseaux social des collectivités, etc.
- Récupération des données des citoyens et analyses des tendances ;
- Détailler le modèle économique de la solution
- Mettre en place une infrastructure technique solide
- Optimiser l'algorithme / programme Big data
- Développer les applis mobile / tablette

2. Chapitre 2 : Comprendre l'action publique à l'ère du Cyber-État

A. L'État et le numérique

Max Weber définit l'État comme : «*toute entreprise politique de caractère institutionnel lorsque et tant que sa direction administrative revendique avec succès dans l'application des règlements le monopole de la violence physique légitime*. »[(1)]. En effet, cette définition donnée par peut être considérée comme un point de départ idéal-typique pour appréhender la nature politique de l'État et de son pouvoir pour exercer le contrôle des flux, d'informations et des territoires ainsi revendiquer son monopole légitime de coercition sur un espace déterminé. Dans cette perspective wébérienne, Carré de Malberg souligne que l'État est : « *une communauté d'hommes, fixée sur un territoire propre et possédant une organisation d'où résulte pour le groupe envisagé dans ses rapports avec ses membres une puissance suprême d'action, de commandement et de coercition* »[(2)].

Cependant, Marx et Durkheim ont une vision différente de l'État. En effet, pour Karl Marx[(3)], L'État est un instrument au service des intérêts de la bourgeoisie, sa genèse historique est liée à l'apparition de la bourgeoisie. Il considère que l'État est une superstructure idéologique et philosophique et qui est déterminée par les rapports économiques entre classes aux intérêts opposés. Emile Durkheim[(4)], quant à lui, a une vision positive de l'État. Il établit une relation entre l'apparition de l'État et la complexification de la société à cause du travail et des rôles sociaux qui se divisent et se diversifient.

Cependant, le rôle de l'État va être central et fera figure de pouvoir selon divers conceptions allant d'une approche démocratique de Locke[(5)], celle despotique de Hobbes[(6)] qui sont venues après les approches de Machiavel[(7)]. Cependant, ce rôle central de l'État va évoluer à travers les années et vise à garantir une sécurité collective qui n'existe pas dans l'État nature où « l'homme est un loup pour l'homme »[(8)]. Ce rôle central joué par l'État est contesté en suspectant l'administration publique d'abus du pouvoir.

---

(1) M. WEBER, Le Savant et le Politique, La Découverte, 2003, p. 17.

(2) C. DE MALBERG, Contribution à la théorie générale de l'État, Tome 1, Librairie de la Société du recueil Sirey, Paris, 1920, p.7.

(3) Voir K. MARX, Contribution à la critique de l'économie politique, 1859.

(4) E. DURKHEIM, Le socialisme. Sa définition – Ses débuts – La doctrine Saint-Simonienne, Paris: Les Presses universitaires de France. 1928.

(5) J. LOCKE, Traité des gouvernements civil (1690), Flammarion, 2000.

(6) T. HOBBES, Leviathan, London, Oxford University Press, 1996.

(7) N. MACHIAVEL, Le prince : Texte intégral et analyse par T. Ménissier, Poche, 2003.

(8) J-J. ROUSSEAU, Du contrat social, Paris, Flammarion, 2001.

En effet, Adam Smith estime que les missions de l'État doivent être avant tout celles « *qu'un particuliers ou un petit groupe de particulier n'aurait pas intérêt à faire ou à soutenir, au dont le profit ne couvrirait pas pour eux la dépense* »[(1)]. Ainsi, il souligne que les missions de l'État qui relèvent de son devoir sont principalement la défense, la justice et les travaux publics.

Cependant, la formation de l'État dans les modèles classiques de Thomas Hobbes[(2)] ou de Jean-Jacques Rousseau[(3)], vise à garantir une sécurité et une liberté qui n'existait pas dans « l'État nature » où l'homme est « *un loup pour l'homme* ». Cette garantie permet de fixer des limites que chaque membre du corps social est tenu de respecter sous peine de sanctions. Il s'agit par là d'une application stricte d'égalité entre les hommes qui constitue le cœur de la démocratie. Une démocratie qui doit être également préservée à l'ère numérique. C'est ainsi que l'intervention de l'État dans le domaine du numérique est aussi suscitée et légitimée par l'intérêt collectif et en particulier par la sécurité physique et « *sécurité numérique*» des citoyens ainsi que par l'égalité des accès aux infrastructures numériques.

En effet, le rôle du contrôle légitime doit être assumé par l'État afin de garantir les conditions nécessaires d'une vie démocratique numérique accessible à tous les citoyens sans aucune forme de discrimination. Pour cela, l'État central, en France mais également au Maroc, joue un rôle essentiel dans la régulation des télécoms, de l'Internet et des domaines informatiques : respect de la législation en vigueur, égalité face au numérique, *etc*. C'est ainsi, que l'État mène des politiques interventionnistes pour définir des normes et assurer la sécurité des citoyens, l'accès équitable et la souveraineté du pays. En effet, son contrôle se déroule principalement à travers des agences gouvernementales comme l'ARCEP[(4)] en France et ANRT[(5)] au Maroc ou directement via le pouvoir législatif en mettant en place des lois liées au numérique comme la loi HADOPI[(6)] ou les deux projets de lois liées au numérique : Loi Macron et loi Lemaire en France[(7)].

---

(1) A. SMITH, An Inquiry Into Nature And Causes Of The Wealth Of Nations, 1776, republiée par Edwin Cannan In University Paperbacks, Methvnen & C, Ltd, London, 1961, P. 10

(2) T. HOBBES, Leviathan, London, Oxford University Press, 1996

(3) J-J. ROUSSEAU, Du contrat social, Paris, Flammarion, 2001

(4) L'Autorité de régulation des communications électroniques et des postes (ARCEP) est une autorité administrative indépendante chargée de réguler les communications électroniques et les postes en France.

(5) L'agence nationale de réglementation des télécommunications (ANRT) est un établissement public marocain visant à réguler les télécommunications au Maroc

(6) La HADOPI est une loi no 2009-669 du 12 juin 2009 qui vise à principalement mettre un terme aux partages de fichiers en pair à pair lorsque ces partages se font en infraction avec les droits d'auteur

(7) Selon plusieurs articles de presse, il devait y avoir deux lois «numériques». L'une signée Axelle Lemaire orientée sur les « droits et libertés Internet » et l'autre portée par Emmanuel Macron et sera portée sur des mesures concernant « l'innovation » dont le numérique

En plus de son rôle interventionniste dans les deux pays, l'État doit faire face à de nouveaux défis particulièrement d'ordre technique qui remettent en question les caractéristiques essentielles d'un État souverain. En effet, l'État dans son modèle comme il est reconnu au niveau internationalement par les termes de la convention de Montevideo du 26 décembre 1933. Ainsi, quatre caractéristiques constitutives doivent être constatées de manière évidente :

- L'existence d'un territoire délimité et déterminé ;
- L'existence d'une population résidente sur ce territoire ;
- L'existence d'une forme minimale de gouvernement ;
- La capacité à entrer en relation avec les autres États.

La Convention de Montevideo sur les droits et les devoirs des États est un traité signé à Montevideo (Uruguay) le 26 décembre 1933 au cours de la septième *Pan-American Conference*. Pendant cette conférence, le président américain Franklin Roosevelt a annoncé la mise en route de la politique de bon voisinage, qui mettait théoriquement un terme à la doctrine du « *Big Stick* »[(1)]. L'accord est signé avec quelques réserves de la part des États-Unis, du Brésil et du Pérou. Cette convention est citée en droit international en particulier pour sa définition d'un État souverain comme respectant les quatre critères suivants : « être peuplé en permanence, contrôler un territoire défini, être doté d'un gouvernement, et être apte à entrer en relation avec les autres États »[(2)].

Cette conception de l'État par Claude Duval et François Ettori, et qui rejoint celle de Weber, est fondamentalement remise en cause avec l'émergence du Cloud Computing et de Big data qui constituent les fondements d'un **Cyber-État** comme nous allons le voir dans la prochaine partie.

---

(1) L'expression doctrine du Big Stick renvoie à la politique étrangère menée par le président Theodore Roosevelt au début du XXe siècle et visant à faire assumer aux États-Unis une place de véritable police internationale.

(2) C. DUVAL et F. ETTORI, « États fragiles… ou états autres ? Comment repenser l'aide à leur développement, notamment en Afrique ? », Géostratégiques n° 25, octobre 2009.

B. De la construction du Cyber-État

a) Contexte

Si nous considérons la conception wébérienne de l'Etat selon laquelle un État souverain repose sur quatre éléments fondamentaux qui sont :

- Tout d'abord, l'État est un *espace géographiquement* délimité ;
- Au sein de cet espace géographique, le caractère institutionnel introduit l'idée de rapports *d'autorité à obéissance* ;
- Ces rapports d'autorité à obéissance au sein de l'espace géographique de l'État sont supposés être *pérennes et durables* ;
- Dans cet espace géographique, l'État a *le monopole de la violence légitime*.

En plus, nous considérons également les différentes caractéristiques constitutives d'un État souverain selon les principes reconnus par la convention de Montevideo du 26 décembre 1933 à savoir :

- L'existence d'un territoire délimité et déterminé ;
- L'existence d'une population résidente sur ce territoire ;
- L'existence d'une forme minimale de gouvernement ;
- La capacité à entrer en relation avec les autres États.

A partir de ces éléments, nous remarquons que la conception classique de l'État s'est transformée avec les technologies numériques, et précisément, avec l'avènement de Cloud Computing et de Big data. En effet, ces technologies ont permis l'émergence d'une nouvelle conception de l'État à savoir le Cyber-État selon les principes que nous allons détailler par la suite.

b) L'aspect géographique délimitée disparait dans le Cyber-État

Considérer un État comme un espace géographique délimité est remis en question suite à la disparition des frontières délimitées, voire terrestres, entre les différents États avec le Cloud Computing et Internet. En effet, les applications mises à disposition dans le Cloud pour les utilisateurs peuvent être assimilées à un *territoire*. Les utilisateurs de ces applications sont considérés comme des citoyens apparentant à ce territoire virtuel, donc des cyber-citoyens. C'est ainsi qu'ils y forment une *population*. Cette population utilise une *monnaie virtuelle* via des plateformes dédiées à l'image de la plateforme Bitcoin[(1)]. De ce fait, les utilisateurs de ses applications, des cyber-citoyens de toutes les nationalités confondues, pratiquent les tâches de la vie quotidienne dans cet espace qui appartient au Cyber-État et qui n'a aucune restriction géographique.

---

(1) Le bitcoin est une devise monétaire tandis que Bitcoin est un système de paiement dans cette devise. Sous ces deux aspects, Bitcoin se distingue des systèmes préexistants sur les points suivants :

Ainsi, au sein du Cyber-État, les utilisateurs peuvent acheter des espaces de stockage (via la solution Dropbox par exemple) et y stocker leurs fichiers électroniques et données personnelles. Cet espace, loué ou acheté dans le Cloud, pourrait être assimilé, dans la vie réelle, à l'appropriation d'un terrain ou à l'allocation d'un local. D'ailleurs, nous retrouvons les mêmes règles d'utilisation dans le monde réel comme dans le monde virtuel pour ces espaces loués ou achetés : Un contrat de location d'un appartement à Paris, ou un acte d'achat d'un terrain à Casablanca.

A cela s'ajoute la mise à disposition des boutiques en ligne hébergées dans le Cloud et qui permettent aux utilisateurs de comparer les prix et d'acheter les produits avec des prix compétitifs. Cet avantage concurrentiel est dû principalement à la localisation géographique des plateformes et la fiscalité du pays d'hébergement comme en témoigne le cas Amazon.fr qui réalise ses ventes en France et paie ses impôts au Luxemburg. L'État perd donc des recettes fiscales ainsi que son contrôle de la fiscalité.

L'aspect géographique est également remis en question au niveau des aspects d'enseignement et de transmission des savoirs. Les plateformes Cloud Computing, en se basant sur des technologies Big data, permettent à des utilisateurs à travers le monde, sans restriction géographique, d'étudier, d'apprendre et de suivre des cours à travers les MOOCs[(1)] sans se déplacer physiquement dans une école ou à une université. En effet, plusieurs universités, compris les plus prestigieuses du monde, proposent des formations diplômantes à travers Internet et des plateformes MOOCs. Toute personne, assidue et impliquée, se voit délivrer un diplôme ou une attestation de réussite délivrée par ces universités.

Les technologies de Cloud Computing et de Big data permettent ainsi le suivi des étudiants, leur notation et leur évaluation. Ces plateformes MOOCs substituent au rôle fondamental de l'État qui ne contrôle plus le contenu des formations ni le droit de regard sur les diplômes et attestations fournies. Cependant, ces plateformes démocratisent l'accès au savoir et décharge l'État de certaines responsabilités. En effet, il suffit d'une connexion Internet pour suivre les meilleurs cours de l'université de Harvard tout en vivant en Afrique.

- Contrairement aux autres devises monétaires, Bitcoin n'est pas l'incarnation de l'autorité d'un État, d'une banque ou d'une entreprise. La valeur du Bitcoin est déterminée de façon entièrement flottante par l'usage économique qui en est fait et par le marché des changes. Les règles organisant l'émission monétaire sont quant à elles déterminées uniquement par un code informatique libre. En tant que système de paiement, il se distingue par le fait que son fonctionnement ne requiert pas l'utilisation d'une infrastructure centralisée tenant les comptes des montants détenus afin d'assurer les transactions. Le rôle de garantie et de vérification existe, mais est attribué toutes les dix minutes environ à un ordinateur du réseau choisi de façon aléatoire. Bitcoin repose sur un protocole cryptographique notamment pour, d'une part, résoudre le problème dit du double paiement, qui avait jusqu'alors empêché l'émergence d'un tel type de monnaie, et pour, d'autre part, garantir l'impossibilité de falsifier les identifiants des parties prenantes et la valeur du stock de bitcoins figurant dans les porte-monnaie électroniques.

(1) MOOC (Massive Open Online Course, MOOC) ou Cours en ligne ouvert aux masses sont des formations ouvertes et à distances. Les participants aux cours, enseignants et élèves, sont dispersés géographiquement et communiquent uniquement par Internet. L'appellation MOOC a été reconnue en entrant dans le Larousse à partir de 2016.

Ainsi, pour ne pas laisser le champ libre aux plateformes américaines, le ministère de l'enseignement et de la recherche français a lancé la plateforme MOOC « *France-université-numérique* » qui vise à la fois à l'exploitation et l'amélioration d'un patrimoine numérique et universitaire français mais également de proposer une offre de formation contrôlée par les autorités françaises. Actuellement, cette plateforme compte une dizaine de formation et compte quelques milliers d'inscrits. Cependant, du côté marocain, nous n'avons identifié aucune initiative gouvernementale dans ce sens. En effet, l'infrastructure numérique universitaire marocaine nécessite une remise à niveau et souffre d'un manque crucial de moyens et de ressources.

Les utilisateurs des plateformes Cloud Computing peuvent avoir une vie sociale à travers les opportunités que proposent les sites de rencontres comme *Meetic.fr* ou des réseaux sociaux comme Facebook. En effet, ces plateformes s'appuient sur des technologies Big data pour permettre aux personnes inconnues mais avec les mêmes affinités de se rencontrer, de se connaitre voire de se marier. D'autres plateformes comme le *boncoin.fr* permettent de revendre ses affaires et de demander un coup de main en contrepartie d'un service de même type. C'est une nouvelle façon de pratiquer sa vie sociale et son voisinage au sein du Cyber-État avec aujourd'hui une volonté française de taxer ces nouvelles cyber-activités.

Nous remarquons que plusieurs activités du quotidien s'effectuent sur Internet et facilité par des technologies de Cloud Computing et de Big data. Ces activités qui relèvent traditionnellement du champ de l'État sont de plus en plus pris en charge par des plateformes Internet dont la majorité est hébergée hors le territoire national français ou marocain.
Nous assistons donc à une disparition des frontières géographiques qui constituent un élément fondamental dans la conception classique de l'État. Ainsi, le Cyber-État prend comme espace non-délimité et sans restriction géographique.

a) L'aspect obéissance à l'autorité dans le Cyber-État

Le rapport d'obéissance à l'autorité de l'État n'est plus garanti à l'ère de Cloud Computing comme il en témoigne les différences des règles juridiques selon le pays d'hébergement de chaque plateforme. En effet, les plateformes Cloud Computing sont soumises au droit et aux règles juridiques de l'État qui les hébergent et non à celui où se trouvent les utilisateurs qui s'y connectent que ce soit au Maroc ou en France.
Ainsi, les différences de législation par rapport aux règles du traitement des données personnelles collectées en est un exemple. En effet, les européens souhaitent intégrer des règles de bonne gouvernance pour l'utilisation de ces données dans le cadre des accords de libres échanges avec les États-Unis. L'objectif recherché est de s'assurer que les citoyens européens obéissent à l'autorité de leur États et non à celles des plateformes Cloud Computing majoritairement nord-américaines.

Ainsi, un utilisateur européen qui utilise une plateforme Facebook ou Gmail subi l'autorité de l'entreprise en question et n'est plus soumis aux lois de son propre pays. C'est ici que l'autorité de l'État disparait et se perd au profit de ce pouvoir récupéré par les plateformes Cloud Computing donc par le Cyber-État.

Nous pouvons considérer également que ces plateformes ont leur propre constitution et leur propre gouvernement. En effet, toutes les plateformes ont une ligne de conduite à respecter via leurs conditions générales d'utilisation (CGU). Ces conditions peuvent être assimilées à une vraie constitution à respecter par l'ensemble des utilisateurs. Mais également, ces plateformes peuvent agir comme un gouvernement qui assure le bon fonctionnement du territoire. Ainsi, Ils peuvent bloquer des utilisateurs, leur retirer le droit d'accès si ils ne respectent pas les règles générales (ou la dite constitution). Elles - les plateformes Cloud Computing - peuvent conduire des « *cyber-politiques-publiques* » et consulter les utilisateurs dans le cadre des politiques d'amélioration de leurs fonctionnalités.

Ainsi, ce rapport d'autorité «*Plateforme Cloud – Utilisateur*» au sein du Cyber-État vient remplacer le rapport classique « *État – Citoyen* » au profit du « Cyber-État – *cyber-Citoyen* ». En effet, l'absence de ce rapport d'obéissance à l'autorité de l'État à l'ère de Cloud Computing et sa situation changeante selon la nature de la plateforme en question montre bien qu'il n'est plus durable et permanent comme le considérait Weber dans sa conception classique de l'État. En effet, le rapport d'un utilisateur européen vis-à-vis une plateforme américaine, régie par une législation américaine, n'est pas le même vis-à-vis une plateforme chinoise, soumise à la législation chinoise. Ainsi, chacune des deux aura sa propre façon de gérer ses utilisateurs et leurs données personnelles.

b) L'aspect de légitimité de la violence par le Cyber-État

Comme nous l'avons vu, l'État a le monopole de légitimité de la violence, une caractéristique qui lui échappe actuellement. En effet, la notion de la souveraineté d'un État est principalement remise en cause et cela précisément depuis la révélation des affaires SWIFT et PRISM par Edouard Snowden. C'est ainsi que le contrôle du territoire et la préservation de la souveraineté politique par l'État est remise en cause avec la diffusion des technologies numériques et précisément le Cloud Computing.

En effet, nous remarquons que les plateformes Cloud Computing ont un pouvoir de coercition et peuvent ainsi jouer le rôle assimilé à celui d'une police dans le monde réel. Ainsi, elles jouent un rôle clé dans le contrôle des contenus diffusés aux utilisateurs, ils contrôlent l'accès à Internet, à l'information et au savoir tout en mettant en place des mécanismes pour favoriser un certain type de contenu à l'aide des technologies de Big data. Elles ont également la capacité à traiter des données personnelles des utilisateurs, à surveiller le comportement des utilisateurs, à les contrôler et à les bannir si ces utilisateurs ne respectent pas la constitution de la dite plateforme. Nous pouvons donc assimiler ces activités aux activités classiques des services de renseignement d'un État.

c) Définition d'un Cyber-État

En nous basant sur l'ensemble des éléments que nous avons présenté précédemment, nous pouvons définir un Cyber-État comme étant une continuité logique de la notion classique de l'État dans le cyberspace.

En effet, nous pensons que la notion classique de l'État doit évoluer et prendre en compte les transformations numériques que connait la société. Ainsi, sa représentation numérique serait assimilée à un Cyber-État qui se base principalement sur des technologies Cloud Computing et Big data. Ainsi, ce Cyber-État confirme sa présence dans un cyberspace mondial et fait respecter les fondements de l'État classique dans ce monde virtuel. Cela passe principalement par :

- Assurer une souveraineté de l'État en développant des plateformes nationales capables de fournir les mêmes services que les plateformes Cloud étrangères ;
- Développer des outils Big data conjugués à des solutions Cloud Computing pour améliorer les services publics fournis aux citoyens à travers Internet ;
- Développer une présence de l'État et l'ensemble de ses administrations sur Internet ;
- Mettre en place des outils Cloud Computing et Big data afin d'assurer la sécurité nationale pour faire face aux programmes de renseignement étrangers, ou de cyber-intelligence.

Ainsi, le contrôle et la surveillance des citoyens, la maitrise de la monnaie et du commerce, la sécurité et la souveraineté du pays, toutes ces activités traditionnellement appartiennent au seul champ d'intervention de l'État ne font que prendre d'autres formes et se font transférer vers d'autres acteurs : principalement des plateformes Cloud Computing dont une majorité sont nord-américaines comme Amazon.fr, Google, Yahoo!, etc. Ce changement profond technique puis technologique qui échappe au contrôle de l'État classique provoque l'émergence d'une nouvelle conception de ce dernier. Ainsi, nous constatons que le concept du Cyber-État prend forme et constitue la prolongation logique de l'État dans le cyberspace mondial. Nous allons détailler les différentes caractéristiques de cette nouvelle notion : le Cyber-État.

C. Champs d'intervention du Cyber-État

Le champ de l'intervention de l'État dans la gestion des affaires publiques est considéré un des champs les plus étendus comme en témoigne l'explosion de la dépense publique générale [(1)] . En effet, en France, cette dépense a dépassé les 53% de PIB pour l'année 2012 (ce taux se situe à 45% en moyenne au niveau de la zone OCDE[(2)]). Ce taux oscillait entre 51 et 56% du PIB depuis 1992 alors que selon un rapport des ministères des finances, *« En 2008 les dépenses publiques progresseraient de 0,9% en volume, marquant un net fléchissement par rapport à 2007.* »[(3)]. Pour le cas du Maroc, cette dépense s'élève à 34,8% du PIB selon les données 2012 de la Banque Mondiale.

Identifier une limite de l'intervention de l'État est difficile à faire malgré les multiples références économiques, juridiques et historiques[(4)]. Ainsi, nous allons essayer de voir s'il est possible de définir une frontière de l'intervention de l'État et de définir les différents champs dans lesquels il pourrait intervenir.

En effet, la distinction entre la sphère publique et la sphère publique sur Internet (ou la « cyber-sphère-publique ») sert fréquemment à comparer les spécificités entre les administrations publiques et les administrations publiques électroniques. Ainsi, souvent cela fait l'objet de luttes permanentes pour promouvoir les différentes conceptions de la modernité. En effet, le secteur public sur Internet (ou le « cyber-secteur-public») est fréquemment rattaché à la flexibilité contrairement à la rigidité du secteur public dans sa conception classique : la lourdeur de procédures administratives par exemple. Cette frontière entre les deux systèmes ne peut pas être linéaire mais elle est de nature mouvante selon la situation et selon le contexte. Il se peut également que cette frontière n'existe même pas, ainsi, la différence entre les deux sphères peut concerner plutôt des démarches réglementées et des démarches non-réglementées. Ou simplement cette distinction permet de différencier les activités régaliennes de l'État des autres activités plutôt marchandes disponibles en ligne sur Internet ou transférables au Cyber-État.

---

(1) Les dépenses sont des paiements en espèces pour les activités d'exploitation du gouvernement pour qu'il fournisse des biens et services. Elles comprennent la rémunération des employés (tels que les paies et salaires), les intérêts et les subventions, les avantages sociaux et les autres dépenses telles que les loyers et les dividendes

(2) OCDE, Panorama des administrations publiques, 2013.

(3) Rapport « Economique, social et financier : Projet de loi de finances pour 2009 », annexe stratégique, Ministère des finances.

(4) L. GUERRE-TALON, « Une frontière public/privé : pour quoi faire ? », Document de recherche CERAM, n°61, 1995.

Pour lever cette ambiguïté entre les deux conceptions du champ public, il serait nécessaire d'adopter des critères qui permettent de classer l'appartenance au champ public classique et voir s'ils sont applicables pour le champ public sur Internet. Cette tâche d'identification des critères n'est pas facile due aux différentes conceptions et définitions du champ public lui-même. Cependant, certains critères convergents sont fréquemment mis en avant. Ainsi, afin d'identifier les activités du champ public, les critères suivants sont à considérer :

- *Il doit y avoir une mission de réalisation des activités ayant un intérêt général et un impact sur le développement social*. En effet, ce type d'activité de l'État est disponible à travers Internet comme en témoigne plusieurs plateformes qui permettent un développement social comme le Volontariat International en Entreprise pour la France[(1)] et le portail Tanmia[(2)] dédiée au développement des associations au Maroc. Par conséquent, le champ public dans le cadre d'un Cyber-État répond bien à ce critère ;

- *Les activités doivent avoir un caractère non marchand et non concurrentiel.* Effectivement, nous remarquons que certaines activités ou démarches publiques disponibles sur Internet permettent la mise à disposition des services de nature non marchandes. Nous considérons donc que le champ public dans le cadre d'un Cyber-État répond également à ce critère;

- *Il doit être contrôlé par l'État*. En effet, l'ensemble des plateformes Internet qui fournissent un service public est fréquemment financé par l'État. Par conséquent, l'État peut contrôler les services proposés sur Internet à travers ces plateformes Cloud formant le noyau du Cyber-État.

Ainsi, à partir de ces éléments, nous considérons que le champ d'intervention de l'État est semblable à celui du Cyber-État. En effet, avec les technologies numériques, le Cyber-État peut avoir les mêmes missions qu'un État malgré la différence des fondements de chacun des deux. Par la suite, nous allons analyser les différentes fonctions du Cyber-État, à savoir les notions du « cyber-secteur public, « cyber-service public » et la fonction publique à l'ère du Cyber-État.

---

(1) www.civiweb.com est un portail gouvernemental qui permet aux jeunes de moins de 28 ans de trouver en mission dans une entreprise française à l'étranger dans le cadre de Volontariat International en Entreprise (VIE).

(2) www.tanmia.ma est un portail gouvernemental qui permet la mise en relation entre les associations reconnues par l'État afin de mettre en place des projets communs de développement.

D. Les services à l'ère du Cyber-État

a) Secteur public à l'ère du Cyber-État

Comme nous l'avons montré dans le précédent paragraphe, la frontière entre le champ d'intervention de l'État et celui du Cyber-État est difficilement identifiable. Par conséquent, donner une définition précise du secteur public est une tâche compliquée et qui ne manque pas de semer quelques ambiguïtés comme le confirment les deux auteurs Romain Laufert et Alain Burlaud: «*Une classification binaire des organisations en public/privé ne correspondant pas à la réalité […] le droit ne permet pas de définir une extension du secteur public d'une façon satisfaisante […]* »[(1)]. En effet, définir une extension du secteur public vers un « cyber-secteur public » à partir des mêmes éléments n'est pas une tâche facile à réaliser.

Ainsi, nous considérons que le secteur public peut-être définit comme l'ensemble des organisations gérées et contrôlées, d'une façon directe ou indirecte, par l'État central ou sa représentation locale. Cette gestion de l'État implique un contrôle de son pouvoir pour l'orientation des objectifs de l'organisation ainsi qu'une gestion, toujours par l'État, des moyens mis à disposition de ladite organisation. Ces organisations comprennent d'une part les administrations publiques de l'État et des collectivités locales, et d'autre part les entreprises dont au moins 51% du capital social est détenu par une administration publique ainsi que les associations qui en dépendent en grande partie pour leur financement.

A partir de ce constat, nous pouvons définir le secteur public au sein du Cyber-État comme étant une extension de l'ensemble des représentations centrales ou locales de l'État dans le cyberspace. Le Cyber-État assure sa domination et son contrôle et oriente le fonctionnement de toutes ces plateformes qui constituent l'extension du secteur public sur Internet. Il s'agit donc ici du « cyber-secteur public ».

Dans le cadre de notre recherche, nous avons noté qu'à travers le projet d'État Andromède lancé en 2011, son ambition est de créer un Cloud « *souverain* » sécurisé pour les entreprises et les administrations françaises[(2)]. En effet, cela s'inscrit dans l'objectif de donner au Cyber-État les fondements nécessaires pour accueillir l'extension du son secteur public, donc développer un « cyber-secteur public ».

---

(1) R. LAUFERT et A. BURLAUD, Management Public, Gestion et Légitimité, Dalloz, 1980.

(2) Les deux projets concernés par la création d'un Cloud souverain sont le projet Numergy et le projet Cloudwatt avec la participation de l'État et des industriels français. Nous y reviendrons en détails dans la section 6 dédié au fondement technique Cloud du Cyber-État. Nous avons également rencontré le directeur technique du projet Numergy.

b) Service public à l'ère de Cyber-État

Jacques Chevalier précise que « *Le service public est un mythe légitimant : Il sculpte l'image d'un État généreux, bienveillant, uniquement préoccupé du bien-être de ses sujets* »[(1)]. En effet, la notion de service public est complexe dans un contexte culturel comme celui de la France ou du Maroc. Ce concept revêt souvent d'un caractère de gratuité.

D'un point de vue historique et juridique, les origines de service public sont anciennes comme en témoigne la décision de Tribunal des conflits de 8 Février 1873 connue sous l'appellation «*l'Arrêt Blanco* » et qui a constitué les bases du droit administratif français[(2)]. Par conséquent, le service public devient le critère de comportement de la juridiction administrative et trouve sa légitimité dans le service rendu au citoyen.

Au-delà de ses fondements juridiques, le service public recouvre toutes les activités d'intérêt générales sous la responsabilité, direct ou indirect, des pouvoirs publics. Cette activité d'intérêt général sous forme de service public, peut être l'objet d'une délégation à travers un opérateur privé via une décision publique.

Il est important de préciser que le service public est une activité et non une structure ou une organisation. En effet, cette notion de service publique a été principalement développée par Léon Duguit[(3)]. Ainsi, Duguit en donne la définition suivante : « *Toute activité dont l'accomplissement doit être assuré, réglé et contrôlé par les gouvernants, parce que l'accomplissement de cette activité est indispensable à la réalisation et au développement de l'interdépendance sociale, et qu'elle est d'une telle nature qu'elle ne peut être réalisée complètement que par les gouvernants est un service public* » [(4)].

En France, mais également au Maroc, il existe des différentes catégories de service public :

- *Les* services dits « régaliens » : Cela concerne les fonctions classiques et traditionnelles de l'État à savoir : la justice, la défense nationale, la police, les finances publiques, etc. ;
- *Les services sociaux et culturels* : Ils concernent notamment l'éducation, la santé, les activités culturelles, etc. ;
- *Les services à caractères économique et juridique connu communément sous « Service Publics Industriels et Commerciaux » (SPIC) :* Ils concernent les services répondants aux besoins fondamentaux de l'État comme l'énergie, les transports, les télécommunications, etc.

[(1)] J. CHEVALIER, Le service public, coll. « Que sais-je ? », PUF, 2ème édition, 1991, P. 3.

[(2)] J-M. PONTIER, les services publics, Hachette, 1996.

[(3)] L. DUGUIT, Traité constitutionnel tome III, 3° édition, 1927, p. 61.

[(4)] L. DUGUIT, Des fonctions de l'Etat moderne, 1894.

Ainsi, nous considérons que le service public est également extensible vers un « cyber-service-public » au sein d'un Cyber-État. En effet, pour qu'une prestation ou activité soit reconnue comme de service public, il existe trois principes de base à respecter selon les lois dites « Louis Rolland »[(1)]. Ces trois principes doivent être également applicables dans le cadre d'un « cyber-service public ». Il s'agit donc, de:

- *La continuité* : Les services publics sont tenus de fonctionner d'une manière régulière et continue. Nous ne pouvons pas imaginer un service interrompu de la police par exemple. En effet, avec des plateformes Cloud, l'ensemble des services proposés sont disponibles d'une façon permanente. Le progrès des architectures techniques permet d'assurer un service sans interruption. Nous parlons par conséquent de la notion de QoS[(2)] ou de SLA[(3)].

- *L'égalité* : Tous les usagers doivent être placés face aux services publics d'une position égale sans discrimination sans avantages particuliers. Il s'agit d'une devise de service public : Tous les citoyens sont égaux et doivent être traités de la même façon. En effet, les applications Internet fournissant un service public ne font pas de différentes entre utilisateurs. Tous ont le même accès avec les mêmes performances et aux mêmes applications. Cependant, les moyens d'accès ne sont pas les mêmes. Il existe des zones désertes en matière numérique, par conséquent, ces services en ligne ne sont pas accessibles à certaines populations. Cette situation existe également dans la vraie vie où certains endroits souffrent de l'absence des services publics comme les déserts médicaux par exemple.

- *La mutabilité* : Les prestations fournies aux usagers doivent être adaptées à leurs besoins. Ces prestations doivent évoluées quand les besoins des usagers évoluent. En effet, l'évolution des services proposés dans le cadre d'un «Cyber-État» suit l'évolution des services dans le monde réel. Ainsi, une loi votée modifiant une prestation de service public sera facilement intégrée dans ce service s'il est proposé par Internet.

Ces trois principes constituent aujourd'hui un socle solide de reconnaissance de « cyber-service public » au sein du Cyber-État.

---

(1) L. ROLLAND, Précis de droit administratif, Dalloz, 1938.

(2) La qualité de service (QDS) ou quality of service (QoS) est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité.

(3) Le service-level agreement, que l'on pourrait traduire en français par « accord de niveau de service », « contrat de niveau de service », « garantie du niveau de service » ou plus simplement « convention de service » est donc un contrat (ou la partie du contrat de service) dans lequel on formalise la qualité du service en question. Dans la pratique, le terme « SLA » est quelquefois utilisé en référence aux modalités et/ou à la performance (du service) tel que défini dans le contrat.

En ce sens, la notion de service public renvoie à des choix politiques pour ce qui concerne ses réalisations et à des dimensions à la fois politiques et socioculturelles pour ce qui touche à ses finalités. Nous retrouvons également ces choix dans le cadre du Cyber-État.

Comme nous venons de le voir, si nous considérons les trois principes du service public (continuité, égalité et mutabilité) d'un prisme numérique, on constate que les outils numériques et précisément la disponibilité des services en mode Cloud Computing accessibles par des applications mobiles permettront d'assurer une continuité de services publics, une égalité d'accès à tous les utilisateurs et une évolution des règles et d'adaptation aux nouvelles exigences légales. Ainsi, plusieurs démarches administratives pourront être accomplies seulement via Internet. C'est déjà le cas de plusieurs activités comme la déclaration des impôts en France. En effet, en 2014, plus de 13 millions de contribuables ont utilisé le service de déclaration d'impôt sur Internet, soit un tiers des foyers fiscaux. Au Maroc, les citoyens peuvent demander leurs passeports depuis Internet sans aucune démarche papier auprès de l'administration marocaine. Cette démarche est totalement dématérialisée et s'inscrit dans l'optique de modernisation numérique de l'administration marocaine.

Dans l'avenir, plusieurs services publics pourront être automatisés et industrialisés et mis à disposition avec une simple connexion Internet de l'utilisateur : C'est donc le « cyber-service public » en marche.

c) La fonction publique à l'ère du Cyber-État

En France, il existe trois familles de la fonction publique issues de la loi de décentralisation de 1982. Comme nous le précise Jean-François Lauchaume : « *Les principes communs auxquels elles sont soumises, la similitude de nombreuses règles rencontrées dans les différentes statuts et leurs unicité d'inspiration, constituent la meilleure explication […] au singulier* »[(1)]. Ces fonctions publiques sont les suivantes : la fonction publique de l'État, la fonction publique territoriale et la fonction publique hospitalière.

Ainsi, le statut des fonctionnaires en France est géré par plusieurs lois[(2)]. En effet, en regardant ces textes, nous remarquons que le fonctionnaire est une personne nommée dans un emploi permanent dans une structure administrative. Il est identifiable par les éléments suivants :

- L'employeur est un organisme public ;
- Permanence de l'emploie : L'emploie est à vie même s' il est à temps partiel ;
- Titularisation dans un grade de la hiérarchie administrative.

---

(1) J.F LACHAUMANE, La fonction publique, Dalloz, 1992, P.26.

(2) Les loi concernées sont : La loi du 11 Janvier 1984 portant statut de la fonction publique d'État ; La loi du 26 Janvier 1986 portant statut de la fonction publique territoriale ; La loi du 9 Janvier 1986 relative aux statuts de la fonction publique hospitalière.

Au Maroc, Le Statut Général de la Fonction Publique (SGFP) remonte aux premières années de l'indépendance (à partir de 1956). Ainsi, ce statut SGFP régit encore, à ce jour, le personnel de l'État et des collectivités territoriales du pays. Cependant, depuis son adoption, le Statut Général de la Fonction Publique (SGFP) a fait l'objet de nombreuses modifications (entre 1958-2011) qui ont porté essentiellement sur des domaines spécifiques comme les services militaires et les services du ministre de l'intérieur. En effet, ce statut SGFP s'applique aux fonctionnaires de l'Etat (services centraux et déconcentrés), collectivités territoriales, certains établissements publics à caractère administratif. Cependant, il ne s'applique pas aux militaires, magistrats, magistrats de la cour des comptes, personnel du parlement, agents d'autorité et aux agents de certains établissements publics.

Comme c'est le cas en France, la constitution marocaine de Juillet 2011 assure un accès égalitaire aux emplois publics, interdit toute discrimination et garantit un travail à vie pour les fonctionnaires de l'État.

Nous avons également remarqué une coopération entre les deux pays en matière de modernisation de la fonction publique comme en témoigne le colloque national du 21 juin 2013 sur la refonte du statut général de la fonction publique qui a connu la participation des dirigeants français et marocains ainsi que les experts de la banque mondiale et de l'OCDE. Un deuxième séminaire de coopération administrative franco-marocaine a eu lieu les 17, 18 et 19 avril 2013 à Rabat dans le cadre de l'arrangement administratif signé en décembre 2012 entre le ministère de la fonction publique et de la modernisation de l'administration marocaine et par le ministère français de la réforme de l'Etat, de la décentralisation et de la fonction publique[(1)].

Cependant, la mise en place des services publics et des démarches administratives sur Internet va profondément impacter le statut des fonctionnaires. Ainsi, la garantie d'un emploi à vie dans le cadre d'un Cyber-État est difficilement tenable. En effet, avec des services disponibles sur Internet, plusieurs tâches administratives seront automatisées. Par conséquent, certains métiers dans la fonction publique seront amenés à disparaitre à l'exception des métiers qui assurent les fonctions régaliennes et qui nécessitent la présence de l'élément humain. Cependant, nous verrons naitre d'autres métiers autour du numérique. Ainsi, le Cyber-État aura besoin des cadres administratifs capables de comprendre à la fois les enjeux du cyberspace et de l'organisation de l'État et ce sont eux qui assureront son bon fonctionnement.

[(1)] Voir les détails sur le portail de la fonction publique en France. Le lien direct http://www.fonction-publique.gouv.fr/fonction-publique/europe-et-international-11 , dernière consultation 14/09/2015.

Avec cette transformation de la fonction publique d'État, ce dernier peut réduire ses dépenses et moderniser son administration. Par contre il perdra son statut comme premier employeur et verra plusieurs services classiques se transformer dans le cadre du numérique. Donc appliquer des politiques économiques spécifiques et dominantes aujourd'hui situées dans l'espace doctrinal dit « néo-libéral »… ou de l'école « classique ».

Pour conclure cette partie et nous avons remarqué que dans le cadre du programme de modernisation de l'action publique en France (MAP)(2007 – 2012) et qui se substitue désormais à la révision générale des politiques publiques (RGPP), une feuille de route de l'administration numérique comprend une dizaine de mesures générales qui permettent d'associer les offres numériques (cyber-service public) à des offres de présence territoriale (service public). Les mesures adoptées dans le cadre de cette charte numérique de l'État sont :

- Mettre en réseau les bases de connaissances « métiers » ;
- Proposer de nouveaux services, notamment sur le téléphone mobile ;
- Réaffirmer et étendre le principe de gratuité de la réutilisation des données publiques (*open data*) ;
- Développer la transparence de l'action publique et l'implication des citoyens ;
- Renforcer la maîtrise et la cohérence des systèmes d'information ;
- Moderniser et mutualiser les infrastructures techniques et numériques ;
- Créer un magasin d'applications partagées du service public ;
- Faciliter l'utilisation, le partage, la sécurisation et l'archivage des données de références.

Nous remarquons à travers ces éléments que le transfert de certaines activités de l'État vers le Cyber-État permet d'améliorer la performance publique et permettre ainsi une potentialisation de l'administration publique. C'est ce que nous allons le voir dans la prochaine partie.

E. Performance et modernisation à l'ère du Cyber-État

a) Qu'est-ce que la performance de l'État

Pour les chercheurs en science politique, le concept de performance est difficile à définir. Il engendre de nombreux débats et n'est pas simple à circonscrire. Cependant, la mesure de la performance dans la gestion publique répond à un impératif démocratique, reconnu par la Déclaration des Droits de l'Homme et du Citoyen du 26 août 1789:

> **Article 14 :**
> *« Tous les citoyens ont le droit de constater par eux-mêmes ou par leurs représentants, la nécessité de la contribution publique (…) et d'en suivre l'emploi (…).*

Par ailleurs, *la société a le droit de demander compte à tout agent public de son administration »*.

En France, la recherche de la performance dans le secteur public, entendue comme l'optimisation des services rendus aux citoyens, a connu différentes étapes depuis l'après-guerre. Ainsi, la plus récente étant la Loi Organique Relative aux Lois de Finances (LOLF), votée en 2001 et mis en œuvre à partir de 2006. Avec cette réforme budgétaire, l'administration est passée d'une logique de moyens à une logique de résultats, étape essentielle de l'amélioration de la performance selon la théorie du Nouveau Management Public (NMP). Ainsi, des méthodes de *management*[(1)] – traditionnellement employées dans le secteur privé – se sont peu à peu répandues dans la sphère publique[(2)]. En effet, cela s'inscrit dans une politique néolibérale qui consiste à réduire l'intervention de l'État dans l'économie et la société.

Le Maroc, quant à lui, fait face à des défis économiques majeurs imposant de suivre des politiques d'amélioration de la performance de son secteur public. En effet, les contraintes de l'OMC (Organisation Mondiale du Commerce), les accords d`association avec l`Union Européenne, les négociations avec les Etats-Unis pour la création d'une zone de libre-échange appellent une mise à niveau de l'économie marocaine et l'instauration d'un État performant à travers plusieurs réformes. A cela s'ajoute des défis politiques pour assurer une plus grande ouverture démocratique, une promotion de la participation des femmes dans la gestion publique, la promotion des Droits de l'homme et implication de la société civile dans la gestion des affaires locales.

Pour répondre à ces défis, le Maroc a institué, par la Constitution de 1996, une Cour des Comptes dont les objectifs ne se limitent pas au seul contrôle des politiques publiques et des établissements publics mais concerne aussi à l'évaluation des résultats attendus. De ce fait, le pays a instauré un système basé sur la gestion de la performance tout en mettant en place une réorganisation des services de l'État et des politiques de déconcentration de la prise de décision et de l'octroi de plus de pouvoir aux acteurs locaux.

---

(1) Le management, issu du français « ménagement », correspond à l'ensemble des techniques de direction, d'organisation et de gestion d'une entité afin qu'elle atteigne ses objectifs. Le management n'est pas à proprement parler une théorie mais plutôt une pratique regroupant un ensemble de savoir-faire techniques et relationnels (S. ALECIAN et D. FOUCHER, Le management dans le service public, Paris, Édition d'organisation, 2002.).

(2) Nous entendons par sphère publique les entreprises publiques et les administrations qu'elles soient centrales, déconcentrées ou décentralisées.

La notion de performance correspond à l'atteinte d'objectifs ou de résultats attendus, et plus largement à la création de valeur. Si dans le monde de l'entreprise, la création de valeur est généralement associée à l'accroissement du profit, elle doit être entendue dans le secteur public comme une optimisation des services rendus aux citoyens[(1)]. En effet, les outils numériques permettent cette optimisation des temps de traitement, une facilité d'accès et une amélioration de la relation administration-citoyen.

Ainsi, si les différentes initiatives de réformes politiques publiques, en France et au Maroc, insistent sur plus de performance des services publics, nous pensons que la réalisation d'un tel objectif s'accompagne avec le développement des services publics proposés sur Internet et ce dans le cadre du développement du Cyber-État. A titre d'exemple, la mise en place des lois « LOLF » a été suivie par un une refonte des systèmes d'informations budgétaire de l'État français. En effet, nous avons eu l'opportunité de travailler sur ce projet pendant 7 mois[(2)]. Nous avons pu comprendre la mise en place des lois « LOLF » et leurs articulations avec les technologies numériques : mise en place d'une application mobile pour déclaration des impôts, ouverture des portails de déclarations des taxes et impôts sur Internet, etc.

b) Modernisation de l'État et les écoles des politiques publiques néo-classiques

Il est difficile de traiter le sujet de modernisation de l'État pour plusieurs raisons liées principalement à l'intersection des domaines concernés à savoir : le domaine politique, le domaine économique et le domaine juridique et le champ des domaines dits « régaliens ».

En effet, la modernisation de l'État appelle à confronter les réformes juridiques, économique et politiques à la pratique réelle du terrain. Ainsi, les termes utilisés pour aborder les questions de modernisation portent de confusion et suscite beaucoup du débat. Ainsi, Luc Rouban et Jacques Ziller[(3)] considèrent qu'il est préférable de parler non pas de « modernisation » de l'administration, qui implique un certain rejet de l'État, mais de « réforme administrative ». Ziller précise que : «*derrière l'idée de modernisation se joue (…) la définition de l'État et de ses missions face au marché* »[(4)].

---

(1) V. GALDEMAR, G. LEOPARD et M. SIMON, Performance, efficacité, efficience : les critères d'évaluation des politiques sociales sont-ils Pertinents ?, CREDOC, Paris, 2012.

(2) Notre intervention dans ce projet de refonte des systèmes d'informations de l'Etat s'inscrit dans le cadre de notre stage de fin d'étude du cycle ingénieur à Télécom SudParis. Le stage a duré 7 mois au sein de l'agence pour l'Informatique de l'État rattaché au ministère des finances.

(3) L. ROUBAN, J. ZILLER, « De la modernisation de l'administration à la réforme de l'Etat », Revue française d'administration publique, n°75, juillet-septembre 1995.

(4) Ziller Jacques, « De la modernisation de l'administration à la réforme de l'Etat », Revue française d'administration publique, n°75, juillet-septembre 1995, P. 413.

Par conséquent, la notion de « modernisation » de l'État apparaît comme une notion fixe à contenu variable. Ainsi, la modernisation de l'administration implique le développement de son infrastructure intellectuelle et la réorganisation de son infrastructure opérationnelle mais également d'une intégration du numérique comme partie intégrante dans les processus de modernisation. Ainsi, à l'image d'un système cybernétique, il existe une hiérarchie des systèmes et des sous-systèmes dans l'administration publique. En effet, l'intégration du numérique pour renforcer le Cyber-État, qu'elle soit réalisée par les administrations centrales, les services déconcentrés ou les agences et opérateurs de l'État, doit impliquer tous les services et tous les niveaux d'administrations de l'ensemble des ministères.

Cependant, le numérique et les technologies de l'information font figure de pistes pertinentes pour la modernisation de l'administration car ils abolissent les contraintes matérielles et peuvent permettre une personnalisation de l'expérience de chaque citoyen avec son service administratif. En effet, la dématérialisation des services est à la fois synonyme de diminution des coûts pour l'administration et de simplification pour l'usager. Pourtant, un service numérique ne saurait remplacer la présence, les conseils et l'humanité d'un agent public. En d'autres termes : les liens sociaux directs.

c) Modernisation de l'État en France

En France, la « modernisation » de l'État et de l'action publique est un sujet récurrent dans les programmes gouvernementaux. En effet, le décret du 30 décembre 2005 est venu créer une direction générale de la modernisation de l'État. Une nouvelle loi[(1)] du 2 février 2007 a été adoptée et concerne la modernisation de la fonction publique. Par la suite, c'est au nom de la modernisation du service public qu'une autre loi[(2)] du 21 août 2007 vient poser le principe d'un service minimum au sein des services publics afin d'assurer la continuité de service comme nous l'avons vu plus-haut.

Ainsi, pour s'adapter aux évolutions du monde et de la société, l'État doit constamment se moderniser en prenant en compte les exigences de chaque époque. En effet, une réforme de l'État doit permettre de rendre l'administration plus efficace et d'améliorer les services rendus aux usagers. C'est dans ce sens que plusieurs dispositifs ont été mis en place pour organiser et stimuler les efforts de modernisation de l'administration publique. Ainsi, nous allons analyser l'articulation de ces dispositifs autour du Cyber-État. En effet, ces dispositifs de modernisation sont :

---

(1) Loi n°2007-148 du 2 février 2007 de modernisation de la fonction publique, *J.O.* du 6 février, p. 2160

(2) Loi n°2007-1224 du 21 août 2007, J.O. du 22 août 2007, p. 13956.

- *Réforme du budget et de la gestion publique (LOLF) :* La loi organique relative aux lois de finances (LOLF) du 1er août 2001 doit conduire les administrations à passer d'une logique de moyens à une logique de résultats. Sa mise en place progressive puis son application depuis le 1er janvier 2006 constitue un défi considérable pour l'État, qui doit adopter un nouveau mode de gestion publique. Ainsi, cette réforme s'est accompagnée par une refonte des systèmes d'information de l'État et de la mise en ligne de plusieurs services administratifs sur Internet permettant de compléter des démarches administratives. Cela s'inscrit donc dans le renforcement de la présence des « cyber-services publics » au sein du Cyber-État.

- *Réforme de l'administration territoriale de l'État* : Face à l'accroissement des compétences des collectivités territoriales sous l'effet des lois successives de décentralisation, les administrations de l'État ont dû s'adapter. En 1992, un profond mouvement de « déconcentration » a renforcé les compétences des services territoriaux de l'État. En 2004, une réforme des administrations régionales et départementales de l'État est engagée, renforçant encore le rôle des préfets. En 2007-2009, une profonde réorganisation des administrations départementales et régionales est accomplie. A partir de 2015, la France entame une importante réforme[(1)] territoriale portée par le chef de l'État qui entend transformer l'architecture territoriale la France. Cependant, au sein du Cyber-État, la notion de territoire disparait et nous passons des systèmes décentrés vers des systèmes centrés où l'État contrôle et surveille l'ensemble des systèmes dont il a le contrôle technique. Ainsi, l'organisation territoriale d'un État serait reproduite dans un Cyber-État via des services régionaux disponibles sur Internet.

- *Gestion des emplois et des compétences* : La fonction publique doit aujourd'hui faire face à la fois à de forts besoins de recrutement pour compenser de nombreux départs à la retraite, et à un renouvellement accéléré des compétences nécessaires pour accompagner les nouveaux enjeux auxquels l'administration publique française doit faire face. En effet, la gestion des emplois, des effectifs et des compétences dans l'administration est souvent considérée comme insuffisante. Ainsi, la réforme de la gestion publique engagée par la LOLF vient combler ce manque. Cependant, l'arrivée du numérique et le passage de plusieurs missions administratives sur le Net implique une reconversion d'un grand nombre de fonctionnaires mais également d'orienter les prochains recrutements vers des métiers considérés « d'avenir » où le numérique est omniprésent. Ainsi, la gestion du Cyber-État aura besoin des compétences et des ressources humaines qualifiées afin d'assurer son bon fonctionnement.

---

(1) L'Assemblée nationale et le Sénat ont adopté le projet de loi portant nouvelle organisation territoriale de la République, après l'accord sur le texte lors de la réunion de la commission mixte paritaire le 16 juillet 2014. Il s'agit du troisième volet de la réforme des territoires, voulue par le président de la République, après la loi de modernisation de l'action publique territoriale et d'affirmation des métropoles et la loi relative à la délimitation des régions.

d) Modernisation de l'État au Maroc

Le traitement des aspects de modernisation de l'État au Maroc consiste à traiter également les processus de la décentralisation. Cette décentralisation consiste à mettre en place un rééquilibrage des pouvoirs constitutionnels au profit du pouvoir exécutif accompagné d'une gouvernance financière décentralisée tout en mettant l'usager au centre de l'action administrative. Ce mouvement de déconcentration et de décentralisation intervient alors que le pays était caractérisé pendant plusieurs années par la centralisation de son administration. En effet, on peut distinguer deux étapes importantes de cette modernisation :

- *1956-1980* : reconstruction, au lendemain de l'indépendance de l'État national chargé principalement de mettre en place les institutions du pays et de mettre en œuvre une politique de développement économique et social ;

- *Depuis 1980* : Des politiques de régulation et de facilitation de l'Etat qui doit aussi être le garant de l'équilibre social et territorial.

Ainsi, l'ambition de l'État marocain en modernisant son administration était de conjuguer une ouverture politique et démocratique avec un développement économique et social. Ainsi, le rôle de l'État central était prépondérant après son indépendance dû spécialement à une idéologie d'interventionnisme de l'État et également à l'absence d'un secteur privé organisé et dynamique. Cependant, à partir des années 80, l'État marocain entame plusieurs réformes de son administration pour répondre aux besoins changeants et pressants des citoyens et adapter ses structures économiques et sociales aux mutations de son environnement. Ainsi, le Maroc pourrait faire face à la pression des organismes internationaux et promouvoir de la sorte le développement de son économie et la démocratisation de sa société.

En effet, la modernisation de l'État au Maroc s'est axée principalement sur trois éléments essentiels, à savoir :

- *La qualité des ressources humaines:* L'institution d'une nouvelle politique de gestion des ressources humaines basée sur la généralisation des référentiels des emplois et des compétences qui permettent d'asseoir une politique de recrutement et de mobilité des fonctionnaires ainsi qu'un nouveau système d'évaluation des agents publics basé sur la performance ;

- *Le bon fonctionnement des structures de l'administration* : Il permet de redéfinir les missions des administrations centrales et redynamiser les rôles des services déconcentrés. Ainsi, ils renforceront leurs relations partenariales avec les activités territoriales, la société civile ainsi que l'ensemble des acteurs locaux. L'objectif est d'optimiser les coûts des prestations et apporter des réponses de proximité aux

besoins de la population comme en témoigne la lettre adressée par le roi à son ministre de l'intérieur pour mettre en place les outils nécessaires pour un système décentralisé :

> « *…ce système [la décentralisation] serait resté incomplet si, parallèlement, nous maintenions notre capitale comme seul centre des décisions administratives. Ce paradoxe, qui aurait vidé de tout contenu réel notre politique de décentralisation, ne nous a guère échappé. Aussi, avons-nous constamment invité nos ministres, au niveau central, d'abord d'avoir des délégations régionales aussi étoffées que possible, puis d'élargir au maximum, sans nuire au bon fonctionnement de l'Administration, les compétences de ces dernières…* »[(1)].

- *La simplicité et la transparence des procédures* **:** Elle vise à améliorer la relation avec le citoyen marocain. Ainsi, l'objectif est d'informer le citoyen sur les différentes procédures et améliorer la transparence de la relation administration-citoyen. En effet, l'utilisation intensive des technologies de communication et d'information a permis de rapprocher l'administration du citoyen tout en dématérialisant un grand nombre de démarches administratives avec un esprit d'éthique de lutte contre la corruption. C'est dans ce contexte que le roi du Maroc en personne dans un colloque dédié à l'éthique dans le service public a déclaré que :

> « *[qu'] un bon service exige un sens de responsabilité qui implique le respect des droits du citoyen en évitant que ne se perdent ses intérêts par la négligence, les tergiversations, les atermoiements et les reports incessants »* [(39)]. Ainsi, comme le souligne Malik Boumediene : « *La modernisation de l'État marocain, et plus particulièrement de son administration, apparaît comme une réalité. Cette modernisation se matérialise par une marche tant vers la déconcentration que vers la décentralisation. La place de l'usager dans ses rapports avec le service public bénéficie également d'une attention particulière. Néanmoins, il existe aujourd'hui des freins à la modernisation. Il ne s'agit pas de les occulter mais de les identifier afin de proposer des pistes de réflexions* »[(2)].

---

(1) H. OUAZZANI, Droit administratif, 2003, p.29.

(2) M. BOUMEDIENE, La question de la modernisation de l'Etat dans le monde arabe : L'exemple du Maroc, Pyramides, 2010, p.152

En effet, à l'ère des nouvelles technologies de l'information et de communication (NTIC), le numérique apparait comme un outil important dans les démarches de modernisation de l'administration publique. Ainsi, en faisant cela, le Cyber-État, dont le Cloud et le Big data sont les piliers, se concrétise et s'affirme face à sa conception classique.

Cependant, cette amélioration de la relation administration-citoyen ou « Cyber-État/Cyber-citoyen » et le transfert permanent des activités vers le Cyber-État permet, dans l'autre sens, de mettre en place des outils de surveillance et de contrôle des citoyens. Ainsi, nous nous considérons que le Cyber-État constitue un terrain spécifique également pour les activités de surveillance et par conséquent de contrôle si ce n'est de limitation ou de perte des droits et de libertés fondamentaux. C'est le sujet de la deuxième section.

3. Chapitre 3 : Les politiques publiques à l'ère du Cyber-État

Dans cette section, nous allons essayer de comprendre le champ des politiques publiques et particulièrement celui des cyber-politiques publiques.

Dans un premier temps, nous essayons de donner une définition d'une politique publique puis à d'introduire un nouveau terme celui de la cyber-politique publique. Nous présenterons par la suite la notion de l'analyse des cyber-politiques publiques et en quoi consiste une telle analyse.

Nous détaillerons par la suite l'approche séquentielle qui permet une analyse de bout en bout d'une cyber-politique publique. Ensuite, nous aborderons les limites de cette approche séquentielle.

Nous verrons également le rôle des acteurs et des groupes d'intérêts dans le cadre d'élaboration des cyber-politiques publiques en France et au Maroc.

Par la suite, nous essayerons de voir le phénomène « d'uberisation » des politiques publiques et comment l'État fait face aux nouveaux problèmes d'un nouveau type.

Pour conclure cette section, nous essayerons de comprendre la démarche d'une cyber-politique publique à travers une étude de cas avec la plateforme Cloud Computing « Uber » pour les taxis. Nous essayerons de comprendre les différentes notions étudiés dans ce chapitre à partir du cas de l'arrivée de la plateforme « Uber » en France et au Maroc : Émergence du problème, inscription sur Agenda, réponse politique.

A. Eléments de définition

a) Vers une cyber-politique publique

Comme nous l'avons décrit dans l'introduction, la politique publique capitalise déjà plus de quarante définitions en 1972. Ainsi, Thomas Dye en donne une définition simple, large en considérant que la politique publique est « *ce que les gouvernements décident de faire ou de ne pas faire* »[(1)]. Patrick Hassenteufel lui précise que « les politiques publiques correspondent à l'ensemble des actions de l'État. L'étude des politiques publiques est donc l'étude de l'État en action »[(2)].

En effet, en partant de ces deux définitions de Dye et de Hassenteufel, nous pouvons considérer que les cyber-politiques publiques correspondent à l'ensemble des actions prises (ou pas) par les gouvernements ou les États pour le développement d'un Cyber-État. Ainsi, pour reprendre les termes de Hassenteufel, c'est donc l'étude du Cyber-État en action. En d'autres termes, les cyber-politiques publiques correspondent aux programmes d'action qu'une autorité publique met en place pour un secteur d'activité particulier au sein du Cyber-État afin de résoudre des problèmes publics et répondre à des attentes des cyber-citoyens.

b) Vers une analyse des cyber-politiques publiques

Au sein de la science politique et de la sociologie, nous remarquons que les politiques publiques couvrent par ses contributions trois aspects fondamentaux : la connaissance, l'action et la formation[(3)]. Ces trois notions, nous les trouvons en permanence dans les champs d'application d'une analyse des cyber-politiques publiques. En effet, l'analyse des cyber-politiques publiques nécessite une *connaissance* d'une cyber-politique-publique, une compréhension de *l'action* du Cyber-État et une bonne *formation* des acteurs associés au développement de ce type de politiques publiques.

D'un point de vue historique, l'analyse des politiques publiques (ou *policy analysis*), a été utilisé en 1930 aux États-Unis par Harold Lasswell[(9)] afin de mettre en place une démarche d'analyse qui va permettre au gouvernement américain de comprendre les choix politiques et de prendre les meilleurs et les plus pertinents comme en témoigne le développement par la suite de la cybernétique par Wiener et le développement d'Arpanet qui était à l'origine de l'Internet d'aujourd'hui.

---

(1) T. DYE, Understanding Public Policy , Englewood Cliffs N.J, PrenticeHall, 1972.

(2) P. HASSENTEUFEL, Sociologie politique : l'action publique, Armand Colin, 2008, p.7.

(3) R. LANDRY, Introduction à l'analyse des politiques publiques, Québec, Presse de L'Université de Laval, 1980.

(4) H. LASSWELL, Psychopathology and Politics, Chicago (Ill.), University of Chicago Press, 1930.

Cependant, la vitesse de diffusion de l'analyse des politiques publiques au sein des différentes nations s'est révélée variable, et étroitement liée à la structure de l'État comme aux modes de raisonnement sur les affaires publiques qui lui correspondant[(1)]. En effet, l'analyse des politiques publiques fait sa rentrée dans le paysage français entre le milieu des années 1970 et le milieu des années 1980 et au Maroc début des 1990 suite aux réformes structurelles de l'État marocain imposées par la Banque mondiale. Cependant, l'adoption de cette démarche importée des États-Unis a mis à mal l'image traditionnelle d'un État uniforme dont les décisions s'imposent à la société[(2)].

En parcourant la littérature des politiques publiques, nous constatons que pour qualifier ce qui est « d'analyse des politiques publiques », une multitude de définitions existent selon le contexte et les objectifs visés par la démarche. Pour Dunn par exemple, il définit le concept « d'analyse des politiques publiques » comme : « *Une discipline appliquée de la science sociale qui utilise de multiples méthodes de recherche et d'argumentation pour produire et transformer de l'information pertinente pour une politique, information qui puisse être employée dans des contextes politiques afin de résoudre des problèmes de politiques-action*»[(3)].

Cette définition de Dunn est représentative de deux aspects fondamentaux que nous retrouvons dans le cadre de l'analyse des cyber-politiques publiques :

- Un caractère pluridisciplinaire de la démarche scientifique qui vise à donner une image plus réaliste de l'action du Cyber-État ;
- Une orientation vers une « boite à outils » d'aide à la décision insistant sur les rapports du pouvoir au sein de l'administration publique en montrant la concurrence entre les différentes organisations administratives au sein du Cyber-État. Prenons l'exemple de préparation en 2015 de la loi liée au numérique[(4)] et dont l'intervention du Premier ministre, Manuel Valls, était nécessaire afin de partager les responsabilités entre celle portée par la secrétaire d'État au numérique Axelle Lemaire et orientée sur les «droits et libertés Internet », et la deuxième portée par Emmanuel Macron, ministre de l'économie et relative à des mesures concernant l'innovation numérique.

---

(1) P. DURAN, Penser l'action publique, Paris, LGDJ, coll. « Droit et Société », série «Politique », 1999.

(2) D. KUBLER et J. MAILLARD, Analyser les politiques publiques, Presses universitaires de Grenoble, 2009, p.8.

(3) W.N. DUNN, Public Policy Analysis: An Introduction, EnglandWood Cliffs, Prentice-Hall, 1981, p.45.

(4) Le volet numérique et économie numérique constituait la substance de la loi Macron 2 en préparation en 2015. En parallèle, la secrétaire d'État au numérique Axelle Lemaire préparait de son côté une loi semblable et touchant aux mêmes aspects que la loi Macron 2. L'intervention de Manuel a permet de trancher au profit de la deuxième loi, celle de Lemaire, et ainsi entériner celle de Macron 2. Les articles économiques de cette dernière ont été par la suite repris dans la loi travail El Khomri en 2016 et la loi Macron 2 n'a plus vu le jour.

Ainsi, grâce à l'analyse des cyber-politiques publiques, nous pouvons mieux comprendre l'intervention de l'État dans la réglementation du Cyber-État, et proposer des cyber-politiques publiques pour répondre à des problèmes sociaux principalement liées au numérique. Comme c'est le cas pour l'analyse classique des politiques publiques, il est nécessaire de bien connaître les mécanismes d'une « cyber-politique » et le rôle des acteurs qui interviennent dans chacune de ces étapes, sans oublier que les cyber-politiques publiques sont déterminées par les mêmes institutions que les politiques publiques dans leur sens classique. Ainsi, ces institutions peuvent manier l'interprétation des problèmes sociaux et les solutions possibles, ce qui peut empêcher le bon déroulement des cyber-politiques-publiques efficientes.

B. L'analyse des cyber-politiques publiques à travers l'approche séquentielle

a) Définition

L'identification d'une politique publique n'est pas aussi simple que le laisse supposer l'apparente « consistance » de l'objet[(1)]. En effet, il est difficile d'identifier le problème nécessitant, si besoin, la mise en place d'une politique publique ou d'une cyber-politique publique afin de répondre à un problème social dans le cadre du Cyber-État.

Ainsi, pour comprendre cette réponse apportée par le Cyber-État, il existe plusieurs méthodes de l'analyse des politiques publiques comme l'approche séquentielle (ou *heuristic approach)*. En effet, cette approche se présente comme une grille organisée en séquences d'actions permettant de diviser un processus du développement d'une cyber-politique publique en étapes distinctes[(2)]. Cette approche couvre tout le spectre du travail d'un décideur public dès l'identification du problème jusqu'à sa résolution. Cette approche était le fruit des travaux d'aide à la décision de Charles Jones[(3)] et Jean-Claude Thoeing[(4)].

Ainsi, nous souhaitons à travers cette approche séquentielle construire un cadre fixe et suffisamment générale pour pouvoir l'appliquer à une cyber-politique publique. Cette dernière constitue un ensemble de mesures concrètes qui forme la réponse du Cyber-État à un problème social identifié, ainsi, permettre donc d'avoir un Cyber-État en action comme le soulignait Hassenteufel[(5)].

---

(1) P. MULLER, De la théorie de l'État à l'analyse des politiques publiques, Que sais-je ? , 2009.

(2) L. BOUSSAGUET, dictionnaires des politiques publiques, Les presses Sciences Po, 2010.

(3) C. JONES, An Introduction to The Study Of Public Policy, Belmont, Wadsworth, 1970.

(4) JC THOEING, M. GRAWITZ et J. LECA, Traité De Sciences Politiques : politiques publiques, Tome 4, PUF, 1985.

(5) P. HASSENTEUFEL, Sociologie politique: l'action publique, Armand Colin, 2008, p.7.

L'approche séquentielle se résume donc en cinq étapes principales qui sont :

1) *Indentification du problème :* Cette étape d'indentification du problème permet au Cyber-État d'agir sur le problème identifié. Cette identification constitue souvent le point du départ d'une cyber-politique publique ;

2) *Formulation du problème :* Une fois le problème identifié, il faut déterminer le public ou les publics concernés. En effet, cela peut concerner seulement les citoyens internautes (donc les cyber-citoyens) utilisant les plateformes mises à disposition par le Cyber-État mais également tous les citoyens qui trouveront la réponse à leurs problèmes via une plateforme Internet mise à disposition, toujours, par le Cyber-État après avoir analysé les causes et trouvé des solutions adéquates. *C'est la phase de formulation* ;

3) *Prise de Décision* : Une cyber-politique publique comprend des décisions qui peuvent être de nature autoritaire confirmant ainsi le rapport obéissance à autorité selon Weber. Il s'agit ici d'une prise de décision parmi une panoplie de solutions possibles. La décision peut concerner une ou plusieurs solutions jugées adéquates ;

4) *Mise en Œuvre* : Une cyber-politique publique s'inscrit dans un cadre général ce qui permet d'identifier une cyber-politique publique d'une simple mesure d'action. Cette mise en œuvre dans un cadre général permet l'application de la décision et sa traduction en actions concrètes par le Cyber-État ;

5) *Evaluation des résultats :* Une cyber-politique publique définit obligatoirement des objectifs à atteindre. Pour vérifier si ces objectifs ont été réalisés, il faut analyser les effets de la cyber-politique publique sur le problème identifié dans la première étape. Ainsi, Il permet de conclure si la cyber-politique publique menée a réussi, ou au contraire, le problème persiste encore et nécessite la mise en place de d'autres cyber-politiques publiques.

b) Schématisation de l'approche séquentielle

Pour bien comprendre l'approche séquentielle, nous schématisons[(1)] donc les différentes étapes de la façon suivante:

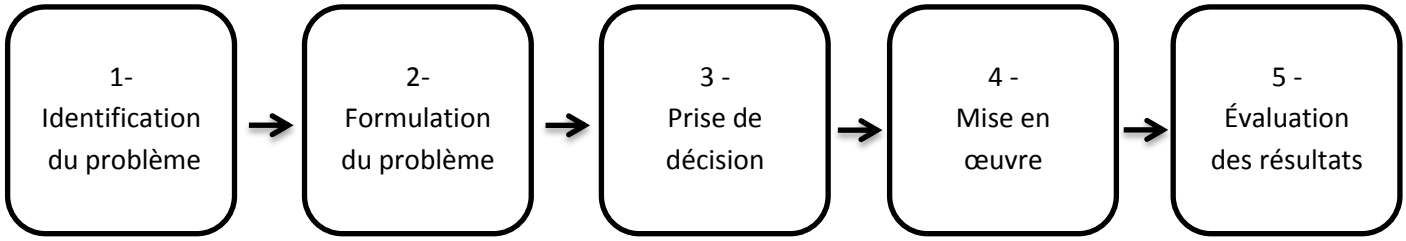


Figure 3 : Schéma représentant l'approche séquentielle d'analyse des politiques publiques

c) Les limites de l'approche séquentielle

Ce type de grille permet d'embrasser de manière particulièrement cohérente les multiples facettes de l'action du Cyber-État et permet de présenter les principaux apports d'un point analytique. Cependant, l'approche séquentielle présente une difficulté de distinguer les différentes étapes dans la réalité et au fait qu'elles soient – les différentes étapes - parfois inversées ou ont entre-elles de nombreux effets de rétroaction[(2)]. Pour y faire face dans le cadre d'une analyse d'une cyber-politique publique, Pierre Muller[(3)] insiste sur le fait que plusieurs précautions doivent être prises pour éviter une approche simpliste des problématiques. Cette approche simpliste risque d'inverser ou perturber les différentes étapes, par conséquent, elles deviennent difficilement identifiables.

Ainsi, selon Charles Lindblom et Edward Woodhouse, « *des étapes ordonnées, cohérentes ne* constituent pas un portrait réaliste du fonctionnement concret du processus de politiques publiques C'est au lieu de cela, un processus complexe et interactif, sans début et sans fin identifiées »[(4)]. De son côté, Sabatier précise que « la conclusion semble imparable : l'approche séquentielle n'est plus heuristique et doit être remplacée avec de meilleurs schémas théoriques »[(5)].

[(1)] Schéma réalisé par nous-même suite à notre compréhension de l'approche séquentielle de l'analyse des politiques publiques. Il n'est donc pas issu d'aucune source bibliographique.

[(2)] D. KUBLER ET J. MAILLARD, Analyser les politiques publiques, Presses universitaires de Grenoble, 2009.

[(3)] P. MULLER, De la théorie de l'État à l'analyse des politiques publiques, Que sais-je ? , 2009.

[(4)] C. LINDBLOM ET E. WOODHOUSE, The policy making Process, Prentice Hall, 1993, p.11.

[(5)] P. SABATIER, Theories of the policy process, Boulder, Wester View Press, 2007, p.7.

Ainsi, les limites de l'approche séquentielle peuvent se résumer dans les points suivants :

- Attribuer un début et une fin à une politique est considéré non réaliste. En effet, toute cyber-politique publique est un flux continu de décisions variées. Les cyber-politiques publiques n'ont pas de date de début ni date de fin ;

- Les étapes se chevauchent entre-elles et la séparation entre ces étapes apparait comme un élément difficilement tenable ;

- Dans le domaine des cyber-politiques publiques, une décision implique d'autres décisions. Dans le schéma de l'approche séquentielle, une décision est isolée par rapport à d'autres ce qui va à l'encontre du principe d'une cyber-politique publique qui souvent impliquent plusieurs décisions ;

- Comme nous l'avons souligné plus haut, l'approché séquentielle suppose une vision rationalisée de l'action publique alors que pendant le processus de mise en place, d'autres problématiques pourront apparaitre ainsi d'autres décisions et d'autres solutions pourront être émises.

Cependant et malgré les multiples critiques à l'encontre de l'approche séquentielle, cette dernière reste un élément essentiel dans le champ d'analyse des cyber-politiques publiques et d'analyse des politiques publiques en générale. En effet, elle met en évidence les différentes phases d'élaboration d'une cyber-politique publique en réponse à un problème identifié. A la fin de cette section et à travers une étude de cas de la plateforme Cloud de mise en relation entre particuliers « *Uber* », nous appliquerons les différentes étapes de cette approche pour comprendre le problème social suscité par ce conflit avec les taxis.

C. Les acteurs dans les cyber-politiques publiques

a) L'acteur dans un processus de décision

Le processus de décision ou de cyber-décision dans le cadre d'une cyber-politique publique est associé à une pluralité d'acteurs ayants des identités différentes et des intérêts divers. Ainsi, les acteurs peuvent être des élus locaux, des experts, des administratifs ou fonctionnaires, des acteurs gouvernements, des plateformes Internet, *etc*. Ainsi, il s'agit de toute personne impliquée dans un processus de décision concernant une cyber-politique publique donnée.

En effet, les analyses portées sur la prise de décision dans un processus de décision d'une cyber-politique publique ont montré la divergence relative aux façons de faire et aux intérêts au sein d'un même groupe : gouvernement, partis politiques, Plateformes Internet,

syndicats, *etc*. En effet, il existe des relations complexes et de rivalité entre les membres des différentes organisations dont les acteurs sont préoccupés par les objectifs de leurs organisations que par les objectifs globaux comme en témoigne la réforme de la taxation des plateformes Internet étrangères. En effet, le gouvernement souhaite la mise en place d'une politique fiscale au niveau européen, le MEDEF et le ministre de l'économie, Emmanuel Macron, craignent la fuite des investisseurs et des startups numériques vers d'autres pays si de telles politiques sont adoptées comme en témoigne ces différentes déclaration en 2015.

Ainsi, dans une démarche de prise de décision dans le cadre d'une cyber-politique publique, l'acteur unique est rarement présent tout seul. Les décisions prises suscitent souvent divergences d'intérêt au sein du même groupe contenant les acteurs engagés. Un groupe d'intérêt pourrait être lui-même acteur dans un processus de prise de décision. C'est ce que nous allons voir dans la suite.

b) Les groupes d'intérêt comme acteurs : Exemple de Syntec Numérique

« *Les groupes d'intérêt sont des organisations qui ont une certaine autonomie vis-à-vis du gouvernement et des partis politiques et qui cherchent à influencer les politiques publiques*»[(1)]. En effet, les groupes d'intérêt font partie intégrante du processus de fabrication des cyber-politiques publiques et ils y occupent une place importance. L'influence de tels groupes, comme CapGemini ou Atos, varie en fonction du contexte politique et de secteur des cyber-politiques publiques concernées.

Pour les autorités publiques, l'objectif recherché via une consultation et une implication des groupes d'intérêts est d'avoir une légitimité de la démarche suivie vu que ces groupes d'intérêts portent souvent les réclamations de la société et de la société numérique dans notre contexte. Ainsi, les autorités entretiennent des relations de proximité avec ces groupes pour profiter de leurs expertises économiques ou légales dans la mise en œuvre d'une démarche de cyber-politique publique. De ce fait, ces groupes bénéficient de cette proximité en faisant passer leurs intérêts en priorité auprès des décideurs publics.

Comme nous le remarquons, les rapports entre décideurs publics et les groupes d'intérêts sont généralement réalisés sous la forme d'un échange dans les deux sens. Un échange qui n'est pas très défini mais qui change selon le contexte et les contraintes de chaque partie. Cette organisation d'échange dans le processus de prise de décision d'une cyber-politique publique a fait naitre une sorte de communauté fermée réunissant des gouvernementaux et des groupes d'intérêts au sein d'un même champ d'application de décisions et de normes. Cette configuration renvoie vers la notion classique du réseau dans la sociologie appelée «les réseaux de politiques publiques»[(2)].

[(1)] L. Wilson, Alternative Models of Interest Intermediation : the Case of France », *British Journal of Political Science*, avril 1982, p. 200

[(2)] P. MULLER, De la théorie de l'État à l'analyse des politiques publiques, Que sais-je ? , 2009.

Ainsi, dans le cadre des cyber-politiques publiques, le groupement Syntec Numérique peut être assimilé à un groupe d'intérêt dans le cadre d'élaboration des politiques publiques impactant le domaine numérique. En effet, Syntec Numérique, créée en 19702 sous le nom Syntec informatique (pour devenir Syntec Numérique en 2010), représente 1 200 entreprises numériques (25 grands groupes, 75 ETI, 800 PME et 300 startups), organisées autour de 3 collèges ; les entreprises du Conseil et Services en Informatique (SSII), du Conseil en technologie et les éditeurs de logiciels et de services Internet. Selon les chiffres publiés en 2015 par Indice Syntec, la filiale statistique de Syntec Numérique, les entreprises adhérentes représenteraient 80 % du chiffre d'affaires qui s'élève à 42,5 milliards d'euros et qui emploie 400 000 personnes salariées.

Ainsi, Syntec numérique, en tant que groupe d'intérêt lié au numérique, possède une mission de porte-parole de son industrie auprès des institutionnels et des pouvoirs publics. Son avis et ses préconisations sont largement pris en compte par le gouvernement dans l'élaboration des cyber-politiques publiques. En effet, sa participation et son influence dans les débats sont significatives comme en témoigne la publication de plusieurs livres comme le Livre Blanc sur le Cloud Computing en mars 2012, le Livre Blanc du logiciel en février 2012, le Livre Vert sur le Green Computing, les centres de traitement de données et le développement durable en juillet 2011 et le Livre Blanc sur l'hôpital numérique en mai 2011[(1)].

c) Acteur clés des cyber-politiques publiques en France

En France, deux acteurs principaux jouent un rôle central dans le fonctionnement des processus de prise de décision. Ces acteurs agissent d'une façon discrète, cependant leur présence est primordiale dans le processus de fabrication des cyber-politiques publiques.

iii. Les cabinets

Ce type d'acteur prend forme d'une « administration d'État-major »[(2)]. En effet, cet acteur se caractérise par trois traits fondamentaux[(3)]:

- Il se développe auprès de tous les décideurs : Chefs de gouvernements, différents ministres, responsables territoriaux, etc. Le ou les cabinets constituent le « Brain trust » (cerveau de confiance) de l'autorité publique dans le processus de prise de décision ;
- Ses membres sont choisis librement par le décideur ou le responsable politique. Ils ne font pas l'objet de création de postes de fonctionnaires ou d'appel à candidature ;
- Il se développe à la frontière de l'administration et de la politique.

---

(1) Tous ces livres blanc sont en libre téléchargement sur le site de Syntec Numérique sur le lien suivant : http://www.syntec-numerique.fr/publications (consulté le 03/09/2016 à 23h)

(2) J-L QUERMONNE et J. QUERMONNE, La haute fonction publique sous la 5eme République, Paris, PUF, 1983.

(3) P. MULLER, De la théorie de l'État à l'analyse des politiques publiques, Que sais-je ? , 2009.

Le cabinet ou l'état-major constitue l'entourage immédiat du ministre, de premier ministre ou du président de la république. Ces membres sont soigneusement choisis. Ces cabinets sont essentiellement l'organe de préparation des décisions mais leur rôle se voit renforcer avec la mise en place du secrétariat générale de la présidence (SGP), du secrétariat général du Gouvernement (SGG), du secrétariat générale des affaires européenne (SGAE) ou finalement le secrétariat générale de la Défense et de la sécurité Nationale (SGDSN).

iv. Les Grands corps

L'importance des logiques dites des « Grands corps » est une spécificité française[(1)]. En effet, les Grands corps se distinguent par le caractère interministériel des fonctions exercées et à l'aptitude des membres du corps qui exerce le même métier à essaimer en dehors des fonctions d'origines au sein des cabinets ministériels, des sociétés nationales, ou dans le secteur privé[(2)].

Nous remarquons que les Grands corps sont principalement placés dans l'inspection des finances, la Cour des Comptes, et le Conseil d'État. Ils sont issus des corps de Polytechniques, ainsi que les ingénieurs des Ponts et Chaussés, des Eaux et des forets et les ingénieurs des Mines et de l'Armement ainsi que l'École Nationale d'Administration (ENA).

Les Grands corps forment donc un réseau qui permet une forte interconnexion entre les différents cabinets ministériels qui, sans doute, permet une meilleure fabrication des politiques publiques. Ce réseau est renforcé également par le caractère d'homogénéité de leur formation de base principalement suivie à l'ENA ou à Polytechnique ou dans d'autres Grandes écoles.

Finalement, avec la notion « d'élite programmatique »[(3)], la capacité de ces différents acteurs, cabinets et grands corps, à se constituer en élite passe par leurs compétences dans l'élaboration et la mise en œuvre des politiques publiques. Cette élite est alors en mesure de faire accepter comme « juste » une représentation adaptée à ses propres intérêts. (Muller, 2009).

d) Acteurs clés des politiques publiques au Maroc

Au Maroc, le pouvoir exécutif est partagé entre le gouvernement et le Palais dans la personne du Roi. Cependant, le pouvoir législatif est partagé entre le gouvernement, et les deux chambres du parlement : la Chambre des représentants et la Chambre des conseillers. L'équivalent de l'Assemblée nationale et le Sénat en France.

---

(1) M-C. KESSLER, Les grands corps de l'Etat, Paris, PUF, 1994.

(2) J-L QUERMONNE ET J. QUERMONNE, La haute fonction publique sous la 5eme République, Paris, PUF, 1983.

(3) W. GENIEYS, Sociologie politique des élites, Paris, Armand Colin 2011.

i. Le Roi comme chef d'État

Selon la dernière constitution marocaine votée en Juillet 2011 et ses différents articles, le roi est le chef politique suprême. Il préside le Conseil des ministres, peut renvoyer n'importe quel ministre, dissoudre le Parlement, suspendre la constitution, appeler pour de nouvelles élections, ou diriger par décret royal. Il est également le chef des armées et chef religieux du pays. Ces fonctions sont assurées par les articles de la constitution suivants :

[Article 41] :
« Le Roi, Amir Al Mouminine, veille au respect de l'Islam. Il est le Garant du libre exercice des cultes. Il préside le Conseil supérieur des Oulémas, chargé de l'étude des questions qu'Il lui soumet. Le Conseil est la seule instance habilitée à prononcer les consultations religieuses (Fatwas) officiellement agréées, sur les questions dont il est saisi et ce, sur la base des principes, préceptes et desseins tolérants de l'Islam. Les attributions, la composition et les modalités de fonctionnement du Conseil sont fixées par dahir.

Le Roi exerce par dahirs les prérogatives religieuses inhérentes à l'institution d'Imarat Al Mouminine qui Lui sont conférées de manière exclusive par le présent article.»

[Article 42] :
« *Le Roi, Chef de l'État , son Représentant suprême, Symbole de l'unité de la Nation, Garant de la pérennité et de la continuité de l'État et Arbitre suprême entre ses institutions, veille au respect de la Constitution, au bon fonctionnement des institutions constitutionnelles, à la protection du choix démocratique et des droits et libertés des citoyennes et des citoyens, et des collectivités, et au respect des engagements internationaux du Royaume. Il est le Garant de l'indépendance du Royaume et de son intégrité territoriale dans ses frontières authentiques …* »

[Article 53] :
« Le Roi est le Chef Suprême des Forces Armées Royales. Il nomme aux emplois militaires et peut déléguer ce droit ».

ii. Le cabinet royal

Le cabinet royal, quant à lui, est composé du Roi et de ses conseillers. En effet le Roi nomme régulièrement des conseillers personnels et cela pour divers domaines tels la politique, l'économie, mais aussi le domaine numérique.

Selon John Waterbury, « *C'est avec Hassan II que le Cabinet royal a pris l'allure d'un shadow cabinet surveillant étroitement les activités du gouvernement, mais au début, il n'avait qu'un rôle réduit et officieux qui se limitait aux conseils et aux informations donnés par une poignée de collaborateurs discrets à un roi encore mal assuré dans ses nouvelles fonctions de chef de l'État*»[(1)]. En effet, le Cabinet royal a été créé en 1950, sous la dénomination « Cabinet

impérial » avant d'être transformé en « cabinet royal ». Le 7 décembre 1955, un dahir fixe sa composition : un Directeur général, un Directeur, un Chef de cabinet, un Conseiller et huit Attachés, soit 12 personnes. Actuellement, le Cabinet royal compte six Conseillers nommés par dahir et une trentaine de collaborateurs chargés de mission en plus des collaborateurs à temps partiel, qui sont souvent détachés auprès du cabinet par d'autres ministères. Ils seraient ainsi 100 à 150 « *cabinards* » à être concernés.

iii. Le Chef du gouvernement

Selon la constitution marocaine de 2011, le Chef du gouvernement est chargé de diriger le gouvernement et de coordonner l'activité des différents ministres. En cas de besoin, il lui faut arbitrer les divergences de vue qui peuvent apparaître entre les ministres à propos de l'interprétation des grandes lignes de la politique gouvernementale ou de ses modalités de mise en œuvre.

[Article 47]

« Le Roi nomme le Chef du Gouvernement au sein du parti politique arrivé en tête des élections des membres de la Chambre des Représentants, et au vu de leurs résultats. Sur proposition du Chef du Gouvernement, Il nomme les membres du gouvernement. Le Roi peut, à Son initiative, et après consultation du Chef du Gouvernement, mettre fin aux fonctions d'un ou de plusieurs membres du gouvernement. Le Chef du Gouvernement peut demander au Roi de mettre fin aux fonctions d'un ou de plusieurs membres du gouvernement.

Le Chef du Gouvernement peut demander au Roi de mettre fin aux fonctions d'un ou de plusieurs membres du gouvernement du fait de leur démission individuelle ou collective. A la suite de la démission du Chef du Gouvernement, le Roi met fin aux fonctions de l'ensemble du gouvernement. Le gouvernement démissionnaire expédie les affaires courantes jusqu'à la constitution du nouveau gouvernement.»

[Article 78]

« L'initiative des lois appartient concurremment au Chef du Gouvernement et aux membres du Parlement. Les projets de loi sont déposés en priorité sur le bureau de la Chambre des Représentants. Toutefois, les projets de loi relatifs notamment aux Collectivités territoriales, au développement régional et aux affaires sociales sont déposés en priorité sur le bureau de la Chambre des Conseillers. »

[Article 90]

« Le Chef du Gouvernement exerce le pouvoir réglementaire et peut déléguer certains de ses pouvoirs aux ministres. Les actes réglementaires du Chef du Gouvernement sont contresignés par les ministres chargés de leur exécution ».

---

(1) J. WATERBURY, « Le commandeur des croyants, la monarchie marocaine et son élite», PUF, 1975.

iv. La Confédération générale des entreprises du Maroc (CGEM)

La Confédération générale des entreprises du Maroc (CGEM) est l'équivalent du Medef en France. En fait, la CGEM est le représentant du secteur privé auprès des pouvoirs publics et des institutionnels marocain. Cette confédération regroupe 88 000 membres directs et affiliés. Ainsi, elle est acteur influent dans l'élaboration des politiques publiques au Maroc et son avis et ses préconisations sont prises en compte par les institutions marocaines. Ainsi, cette confédération négocie avec le gouvernement en tant que groupe d'intérêt et veille à assurer un environnement économique favorable pour le développement des entreprises adhérentes dont les entreprises numériques.

D. Vers une « *Uberisation* » des politiques publiques ?

En transformant des particuliers possédant un véhicule en chauffeurs occasionnels sans statut, l'entreprise « Uber » suscite des débats autour de la capacité des autorités publiques à apporter des réponses aux nouvelles contraintes sociaux associées au développement des technologies de Cloud Computing et de Big data. En effet, le nom « Uber » est associé désormais au lien entre les technologies numériques et la transformation de chaque secteur d'activité dont les politiques publiques. On parle alors « d'uberisation » des politiques publiques. En effet, le succès des entreprises Cloud Computing et Big data s'accompagne d'une vague de déréglementation poussant les dirigeants politiques à prendre la main et développer des politiques publiques associées comme réponse à ses nouveaux enjeux. Ainsi, au-delà du cas des taxis, c'est toute l'économie des services qui est face à cette révolution aux conséquences sociétales incalculables. D'autant plus que dans une économie de service comme la France ou le Maroc, « l'uberisation » est finalement plus dangereuse que la robotisation des métiers productifs. En effet, le phénomène « Uber » n'est que le début des transformations à venir dont l'emploie serait très impacté. En effet, d'un côté, les plateformes Internet créent quelques emplois ultra-qualifiés, d'un autre, elles en détruisent massivement en prenant des parts de marché à des concurrents traditionnels. Ainsi, il est fort probable que le modèle social actuel soit remis en cause au détriment d'un autre qui va s'appuyer sur des allocations, une assurance-maladie et un RSA d'un nouveau genre. C'est ainsi que le philosophe allemand Byung-Chul Han[(1)] y voit la destruction de toute cohésion sociale qui va laisser chaque homme seul, dans un monde précaire et déloyal.

[(1)] B.H. HAN, Réflexions sur le numérique, Actes Sud Editions, Questions de Sociétés, 2015.

Cependant, une crise comme celle des taxis constitue paradoxalement une opportunité expérimentale pour observer ou repenser la reformulation ou l'évolution du rôle de l'État vers une Cyber-État comme celles de la politique publique vers une cyber-politique-publique. En effet, les institutions publiques doivent choisir un mode de fonctionnement axé sur l'innovation numérique pour faire face au défi d'une dérégulation-régulation numérique, de rendre à chacun la propriété de ses données, de favoriser les échanges équilibrés, de former et de réorienter ceux dont les métiers seront mis en cause par les nouveaux usages. C'est ainsi que les cyber-politiques doivent être considérées comme une priorité et un enjeu de survie pour toute l'institution publique.

E. Comprendre la cyber-politique publique à travers le cas « Uber »

a) Choix du cas de la plateforme « Uber »

i. Objectifs

Nous allons essayer à travers le cas de la plateforme « Uber » de comprendre le processus de mise en place d'une cyber-politique publique. En effet, nous analyserons l'émergence du problème social « Uber », puis la mobilisation des acteurs et la médiatisation du problème en passant par son inscription à l'agenda politique jusqu'à la mise en place d'une loi dédiée à la régulation de l'activité. Nous avons choisi de travailler sur le cas de la plateforme « Uber » pour les raisons suivantes :

- C'est une plateforme Cloud Computing disponible sur mobile (smartphone) et exploitant des technologies Big data. Elle s'inscrit donc pleinement dans le cadre des technologies traitées dans nos travaux de recherche ;

- Elle représente les différentes étapes d'élaboration d'une politique publique : de l'émergence d'un problème jusqu'à la mise en place d'une solution par les pouvoirs publics ;

- Elle est représentative de la transformation numérique et permet de comprendre le rôle des autorités publiques dans la gestion du phénomène dérégulation-régulation provoqué par le numérique ;

- Elle permet de mesurer le degré de flexibilité des textes et lois vis-à-vis du numérique et la façon dont ces derniers doivent ou devraient évoluer ;

- Les mêmes contraintes rencontrées en France avec le cas « Uber » sont reproduites également à l'entrée d'« Uber » au Maroc. Cela va nous permettre également de mesurer la flexibilité du contexte marocain et le comparer au contexte français.

ii. Contexte du conflit

Le conflit qui oppose la société américaine « Uber » aux chauffeurs de taxi en France, au Maroc mais également dans la plupart des pays du monde est un exemple concret d'émergence d'un problème social provoqué par une technologie telle que le Cloud Computing.

En effet, Paris est la première ville hors des États-Unis à accueillir le service d'« Uber ». Son arrivée s'inscrit dans un contexte de libéralisation du transport de personnes en France. Ainsi, le 22 juillet 2009 a été votée la loi mettant fin à la notion de grande remise au profit de la réglementation d'exploitation de voitures de tourisme avec chauffeur (VTC). En effet, en Simplifiant les règles qui réglementent le transport haut de gamme, cette nouvelle loi ouvre la voie aux voitures de tourisme avec chauffeur pour exercer le métier de transporteur aux côtés des taxis classiques.

Ainsi, ce conflit entre taxis et la plateforme « Uber » était largement médiatisé et suivi par l'opinion publique. Sa gestion est remontée au plus haut niveau de l'État, jusqu'au Président de la république lui-même qui a déclaré que « *UberPOP doit être dissous et déclaré illégal et la saisie des véhicules devra être prononcée et effectuée*.»[(1)]. Mais également, les instances européennes ont saisi le problème et ont commencé à réfléchir à des règles communes afin de régulariser ce type d'activité toute en respectant le droit de la concurrence et encourager l'innovation dans l'ensemble des secteurs. [(2)]

« Uber » n'est qu'un exemple. Cependant, les pouvoirs publics vont faire face de plus en plus à ce type de conflit, d'où la nécessité d'anticiper la réglementation tant au niveau technique qu'au niveau juridique.

iii. Lancement du service « Uber »

Uber, est une entreprise technologique qui développe et exploite des applications de mise en contact d'utilisateurs avec des conducteurs réalisant des services de transport. L'entreprise est basée dans la ville californienne de San Francisco, aux États-Unis. En 2015, elle est valorisée à 50 milliards de dollars et ses applications sont commercialisées dans plus de 250 villes dans le monde. Engagée dans un développement rapide, à la fois géographique et via la gamme des services proposés, la société « Uber » a vu son activité interdite dans plusieurs villes du monde.

---

(1) Article publié sur Le Lab Politique Europe, le 26 juin 2015. Disponible directement sur : http://lelab.europe1.fr/taxis-vs-uber-pour-francois-hollande-uberpop-doit-etre-dissous-et-declare-illegal-1360954 . (Dernière consultation 31/08/2015 à 17h).

(2) voir article dans les echos du 28/08/2015. (Dernière consultation 31/08/2015). Il est disponible directement sur : http://www.lesechos.fr/monde/europe/021288655678-confrontee-au-dilemme-uber-lue-va-lancer-une-etude-1148631.php

La plateforme « Uber » est une plateforme Cloud Computing disponible sur téléphone mobile et exploitant des technologies Big data. Elle fait partie de l'ensemble de ces entreprises numériques qui font l'objet de nombreuses polémiques, en raison de débats sur leurs pratiques, vis-à-vis des réglementations sociale, fiscale et administrative en vigueur.

b) Emergence du problème « Uber »

Toute politique publique est issue d'un problème social identifié mais dont les origines ne sont pas forcément connues. En effet, les autorités publiques se saisissent de ces problèmes sociaux en essayant de mettre en place une politique publique associée. Ce travail d'élaboration d'une politique publique comme réponse à un problème ne se fait pas sans une inscription de ce problème sur l'agenda politique.

En effet, en décembre 2011, la société « Uber » annonce son lancement en France comme sa première destination hors des États-Unis. Cette introduction s'inscrit dans un contexte de libéralisation du transport de personnes. Ainsi, dès son arrivée, une soixantaine de voitures de tourisme avec chauffeurs (VTC) sont enregistrées sur l'application proposée par l'entreprise et commencent à circuler pour concurrencer les taxis classiques.

Fort de ce succès, « Uber » élargi son offre et propose à chaque citoyen de pratiquer le métier de taxi via l'application « UberPOP ». En effet, elle permet à des conducteurs particuliers d'être contactés par des usagers pour des trajets urbains tarifés moins chers et sans condition de sélections excepte avoir un âge minimum (21 ans), la possession d'un permis B depuis 1 an minimum. Cette offre permet donc à tout individu possédant un permis de conduire de pratiquer le métier du taxi.

C'est ainsi, que « Uber » a développé son offre de taxi et propose un ensemble de solutions à destination des particuliers mais également des entreprises à des prix très bas ce qui est considéré par les autres taxis comme une concurrence déloyale. A cela s'ajoute les critiques de son montage financier complexe, qui permet à la société de ne pas payer ses impôts et taxes en France à l'instar d'Apple, Google, Amazon ou encore Yahoo![(1)]

Ainsi, pour résumer, les offres proposées par « Uber » pour transformer le secteur du transport des particuliers sont les suivantes (ce ne sont que des applications informatiques dans le Cloud) :

[(1)] Voir Journal De l'Economie, 22 février 2014, Uber : le géant du VTC adepte de l'optimisation fiscale, disponible directement sur le lien : http://www.journaldeleconomie.fr/Uber-le-geant-du-VTC-adepte-de-l-optimisation-fiscale_a669.html. Dernière consultation le 31/08/2015 à 17h.

- *UberX* : chauffeurs professionnels proposant des berlines standards ;
- *Uber Berline* : chauffeurs professionnels proposant des berlines de luxe ;
- *Uber for Business :* permet aux entreprises de payer les déplacements professionnels de leurs employés ;
- *UberPOP* : conducteurs particuliers occasionnels au volant de leur véhicule personnel;
- *UberPool* : permettant de partager son trajet avec un autre passager situé au même endroit et allant dans la même direction, grâce à des conducteurs particuliers occasionnels au volant de leur véhicule personne.

C'est ainsi que le problème « Uber » commence à attirer l'attention des autorités. En effet, les autorités publiques ne peuvent pas mettre sur l'agenda l'ensemble des problèmes sociaux car « *l'attention publique est une ressource rare, dont l'allocation dépend de la compétition au sein d'un système d'arènes publiques […] les problèmes doivent lutter pour occuper un espace dans les arènes publiques. Cette compétition est permanente ; [ils] doivent à la fois lutter pour entrer et pour rester sur l'agenda public* »[(1)]. Et c'est ainsi que le conflit va suivre le processus d'inscription sur agenda politique à savoir : La mobilisation, médiatisation, puis récupération politique jusqu'à la modification de la norme en vigueur[(2)].

c) Mobilisation des taxis classiques

En effet, l'initiative de mobilisation autour d'un problème social dans les politiques publiques revient à des groupes plus ou moins fortement organisés, porteurs d'intérêts socio-professionnels qui se mobilisent le plus souvent de façon conflictuelle avec les autorités publiques. Cette mobilisation vise à gagner le soutien de l'opinion publique afin d'obliger le gouvernement d'agir.

En effet, Pour faire face à cette concurrence qualifiée de « déloyale », plusieurs manifestations et blocages des routes ont eu lieu dans plusieurs villes de France afin que les pouvoirs publics se saisissent du problème et proposent une solution. Ainsi, les chauffeurs de taxis ont organisé une grève générale le 13 janvier 2014. Cette grève a paralysé le trafic routier à Paris, Bordeaux, Marseille, Montpellier et Lyon. Plusieurs manifestations ont suivi par la suite et plusieurs incidents ont été signalés comme agressions des chauffeurs VTC ou des voitures brulées.

---

(1) S. HILGARTNER et C. BOSK, « The Rise and Fall of Social Problems: A Public Arena Model », American Journal of Sociology, vol. 94, n° 1, 1988. , p. 53-76.

(2) Il s'agit de la loi n° 2014-1104 du 1er octobre 2014 relative aux taxis et aux voitures de transport avec chauffeur apparu sur le JORF n°0228 du 2 octobre 2014

d) Médiatisation du conflit

Le conflit opposant la société « Uber » aux taxis traditionnels a attiré l'attention du public. En effet, le métier du taxi est très réglementé et chacune de leur manifestation attire l'attention du public vu son impact sur le quotidien : blocage des routes, difficultés de déplacements, *etc*.

A cela s'ajoute la couverture médiatique associée par les télévisions, les journaux et les plateformes réseaux sociales qui sont devenus un nouvel espace de médiatisation des problèmes sociaux.

Ainsi, les médias ont joué un rôle important en imposant certains champs d'action au gouvernement et ont permis d'inscrire le problème dans l'agenda politique afin de trouver une solution au conflit.

e) Réponse politique

La première réponse politique au conflit consiste à l'instauration au 1er janvier 2013 d'un délai de 15 minutes obligatoires entre la commande et la prise en charge de l'usager pour les taxis avec chauffeur utilisant les applications « Uber ». La mesure devait entrer en application au 1er janvier 2014. Cependant, l'Autorité de la concurrence a rendu un avis négatif à propos de ce décret qui est finalement suspendu en février 2014 pour un problème de distorsion de la concurrence.

Par la suite, le gouvernement a adopté une nouvelle loi dite « *Loi Thévenoud* »[(1)] pour prendre en compte les différentes revendications d'Uber, VTC et les taxis. Ainsi, cette loi a pour objectif de réguler le marché et contrer particulièrement l'offre UberPOP ouvert à toutes les personnes. Le décret d'application de cette loi Thévenoud parait le 30 décembre 2014 au Journal officiel. La principale obligation pour les chauffeurs est de justifier d'un certificat d'assurance pour le transport de personnes à titre onéreux mais cette obligation ne rentre en vigueur qu'au 1er Juillet 2015 et une formation à partir de 2016. Ce décret instaure également une amende à l'encontre des conducteurs de véhicules à titre onéreux qui exercent leur activité sans avoir de carte professionnelle (ce qui s'applique aux chauffeurs UberPop car ils ne sont ni taxi, ni VTC). Mais ce décret est en cours de contestation par la société Uber devant la justice administrative.

Cependant, « Uber » a critiqué la conformité de cette loi à la constitution. Ainsi, la Cour de cassation, le Conseil d'État et le conseil constitutionnel ont été saisi sur le volet VTC de cette loi. Ce dernier a rendu sa décision le 22 mai 2015 en invalidant partiellement loi Thévenoud et en limite la portée.

[(1)] La loi vise à redéfinir les contours de la profession de taxis, à la moderniser et à définir l'usage des véhicules de transport avec chauffeur (VTC). Le texte intégrale est disponible directement ici http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029527162&categorieLien=id.

f) Lancement de la plateforme « Uber » au Maroc

Comme dans des dizaines d'autres villes du monde, « Uber » a lancé son service le 21 juillet 2015 à Casablanca pour une phase de test avant d'élargir le lancement d'une façon officiel et l'échelle de d'autres villes comme en témoigne la directrice générale « d'Uber » Maroc : « *lors de cette phase initiale, nous analyserons nos opérations sur le terrain et procéderont aux ajustements nécessaires, afin de mieux servir les casablancais.* » Elle ajoute que « *A Casablanca, il ne s'agit donc que d'une « phase de test » avec un service restreint* […] *Nous offrons un service complémentaire aux taxis traditionnels afin d'offrir plus de choix aux Casablancais et aux touristes de loisir et d'affaires.* »[(1)]

Ainsi, « Uber » proposera au Maroc son offre de base dans un premier temps à savoir « UberX » qui met à disposition des VTC « *dans le cadre d'un partenariat avec des sociétés de transport touristiques ayant leur propre licence ».* [(2)]

Cependant, la préfecture de Casablanca juge l'activité « d'Uber » Maroc illégale et promet des sanctions aux contrevenants à la loi. Ainsi, dans un communiqué relayé par l'agence officielle Maroc Agence Presse (MAP) le 4 août, la préfecture de Casablanca juge l'activité de « Uber » au Maroc illégale. Selon la préfecture, « *la société n'a fait la demande d'aucune licence régie par la loi* ». « *L'activité « d'Uber » Maroc n'est pas autorisée et expose toutes les personnes qui y travaillent ainsi que les chauffeurs à des sanctions administratives et juridiques* » précise encore le communiqué. La préfecture assure qu'elle prendra « *toutes les mesures nécessaires pour garantir la paix sociale dans le secteur des transports* ».

---

(1) Entretien accordé par Meryem Belqziz, directrice générale d'Uber Maroc au site d'information marocain Médias24. Il disponible directement sur : http://www.medias24.com/SOCIETE/156633-Uber-s-implante-au-Maroc-et-se-lance-a-Casablanca-dans-une-phase-de-test.html.

(2) Entretien accordé par Meryem Belqziz, directrice générale d'Uber Maroc au site d'information marocain Médias24. Il disponible directement sur : http://www.medias24.com/SOCIETE/156633-Uber-s-implante-au-Maroc-et-se-lance-a-Casablanca-dans-une-phase-de-test.html. Dernière consultation le 31/08/2015 à 18h30.

Une situation contestée par « Uber » qui estime que « UberX » est « *un service de mise en relation entre des particuliers et des professionnels du transport via une application. « Uber » ne détient pas de voitures de transport et n'embauche pas de chauffeurs. Ce sont nos partenaires qui détiennent les licences de transport délivrées par l'État. ».* Cependant, la société « Uber » pour légitimer sa présence au Maroc et précisément à Casablanca, elle joue la carte de la sécurité dont souffre le milieu urbain casablancais. En effet, les dirigeants marocains de la société californienne estiment que les utilisateurs sont pris en charge en toute sécurité contrairement aux taxis traditionnels. Meryem Belqziz précise que « Chaque passager pourra envoyer à une personne de son choix par SMS les détails de son trajet (numéro d'immatriculation de la voiture, informations sur le chauffeur, heure présumée de l'arrivée). Les chauffeurs choisis travaillent pour des entreprises de transport touristique. Nous vérifions leur casier judiciaire et demandons leur fiche anthropométrique. En plus, nous disposons de tous les détails des trajets, ce qui rend très facile de retrouver quelqu'un en cas de problème »[(1)].

Ainsi, la société « Uber » s'implante au Maroc et risque de provoquer une révolte sociale et une atteinte à la cohésion sociale marocaine si les autorités publiques n'apportent pas une réponse sachant que le secteur en question emploie des centaines de milliers de familles marocaines qui voient la réduction de leurs ressources qui sont déjà assez bas dans ce secteur d'activité.

---

(1) Déclaration donnée au journal marocain HuffPost Maroc le 20/07/2015. Texte complet sur le lien : http://www.huffpostmaghreb.com/2015/07/20/uber-maroc-casablanca_n_7834994.html, (dernière consultation : 03/09/2015, à 20h)

Partie 2

La société numérique à l'ère du Cyber-État

II. Partie 2 : La société numérique à l'ère du Cyber-État

1. Chapitre 1 : La société numérique à l'ère du Cyber-État

Aujourd'hui, Internet, le Cloud, Big data et l'ensemble des appareils associés (smartphones, tablette, ordinateurs, …) offrent aux individus des possibilités de sociabilité croissante en offrant une « *vie numérique* » qui constitue le prolongement de la vie réelle. Cette vie numérique est moins riche vu que seules les symboles (lettres, mots, signes, …) qui sont échangés. En effet, à l'heure actuelle, on ne peut pas encore y transmettre des odeurs par exemple. En contrepartie, les applications disponibles dans le Cloud Computing permettent de stocker ces symboles en créant ainsi un grand réservoir de données accessible facilement.

La vie numérique des individus a évolué en parallèle de l'évolution de la technologie qui permettait la multiplication des formes d'interaction. En effet, le courrier électronique est apparu en 1970 avec le projet Arpanet[(1)] et le MINITEL[(2)] en France. Puis les forums ont vu le jour dès les années 80 essentiellement grâce à l'Usenet[(3)]. Quant à la messagerie instantanée, les blogs et les wikis, se sont développés pendant les années 1990s. Puis, les plateformes de contenu (YouTube par exemple) et des réseaux sociaux sont arrivés début des années 2000s accompagnés d'un développement croissant de Cloud Computing et des technologies Big data.

Tous ces dispositifs sociotechniques représentent les innovations qui poussent la sociabilité en ligne. Dans ce chapitre nous allons aborder les points principaux suivants :

- La vie en ligne à l'ère de Cyber-État : nous essayerons de comprendre la contribution volontaire de chacun au développement des savoirs et connaissances partagées. Ainsi, comprendre les motivations des individus pour contribuer à la construction d'une connaissance partagée à travers un ensemble de communautés organisées en ligne ;

- L'identité numérique ou la cyber-Identité: Comprendre cette expression de soi à travers des blogs, des réseaux sociaux visant à développer une sociabilité en ligne ;

---

(1) Pour rappel, Arpanet est le projet à l'origine de l'Internet. Nous l'avons vu au chapitre précèdent et encore traité dans le chapitre suivant.

(2) Le Minitel (pour « Médium interactif par numérisation d'information téléphonique ») désigne un type de terminal informatique destiné à la connexion au service français de Vidéotex baptisé Télétel, commercialement exploité en France entre 1980 et 2012

(3) Usenet est un système en réseau de forums, inventé en 1979 et permet d'utiliser les forums d'une façon simplifier mais moins riche. Il est encore utilisé à ce jour et accessible par Internet.

- Les problématiques du traitement des données personnelles ainsi que toute la législation associée ;

- Nous analyserons les contributions de plusieurs institutions dans ce débat lié à la vie social en ligne : CNIL, CNDP, G29, Chaire de recherche de l'Institut Mines-Télécom « Valeurs et politiques des informations personnelles » et la « Quadrature du Net ».

A. La vie en ligne à l'ère de Cyber-État

L'internet est né dans une communauté d'informaticiens voués à la publication et le partage de leurs connaissances et leurs savoirs. Ces connaissances sont généralement déposées sur le Web ce qui est accroit la richesse de l'Internet. Ainsi, à titre d'information, le site www.worldwidewebsize.com; qui permet d'estimer le nombre de pages web indexées par Google, Yahoo! et Bing ; estime qu'en Août 2015, ce nombre atteignait 50 milliards de pages. Or il existe un nombre important de pages qui sont cachées à ces moteurs de recherche (des pages Facebook par exemple). Par conséquent, le web total est sans aucun doute plus important.

Toute cette connaissance est mise à disposition des Internautes en libre accès dans la majorité des cas. Ce libre accès a créé une « culture de gratuité » que certains, spécialement les médias, déplorent car ils ont des difficultés à valoriser leurs propres contenus : les journaux par exemple.

Cette mine de connaissances se décline en multitude de sites web qui héberge chacun une communauté de contributeurs, de lecteurs, de correcteurs. Cette production reste un phénomène social et culturel et soulève trois types de questionnement :

- Pourquoi les individus participent et contribuent gratuitement à l'alimentation de ces bases de connaissances sur Internet ?

- Comment ces communautés sont organisées ?

- Est-ce que le Cloud Computing favorise-t-il ce type de communauté ?

Pour répondre à ces questions, nous allons d'abord classifier ces communautés dans un premier temps. Puis dans un deuxième nous analysons la motivation des individus à contribuer à ce type d'initiative puis nous analyserons l'impact de Cloud Computing sur la constitution de ces communautés.

En effet, une communauté contributive est un ensemble des individus partageant la volonté de partage de connaissance et de sa mise à disposition des autres individus. Selon Michel Gensollen[(1)], on peut distinguer plusieurs familles de communautés définies par la nature de ce qu'elles partagent :

- *Les communautés d'expérience* qui visent à échanger des opinions sur des biens d'expériences : la musique, bien matériels, séjours touristiques, … . La contribution est relativement simple et subjective. Cette communauté se regroupe autour des plateformes visibles mais la variété des biens fait qu'il est difficile de rassembler tous les objets dans une même plateforme ;

- *Les communautés de pratiques* qui partagent une passion commune où le savoir-faire joue un rôle principal comme le bricolage par exemple. Dans cette communauté, on distingue deux types d'acteurs : les novices et les experts qui se rencontrent à travers une plateforme centralisée. A noter que les efforts fournis par les novices sont limités en comparaison aux efforts des experts qui n'ont d'ailleurs pas beaucoup de temps et de disponibilité. Cette communauté apporte beaucoup aux profils des novices ;

- *Les communautés de partage* de biens numériques qui visent à partager essentiellement des fichiers numériques : vidéos, films, musiques, etc. Dans ce type de communauté, les individus sont à la fois fournisseurs et consommateurs (réseaux P2P) [(2)]. A noter que la part des consommateurs est beaucoup plus importante que celle des fournisseurs ce qui pourrait déstabiliser le fonctionnement de la communauté ;

- *Les communautés épistémiques* qui visent à construire un savoir commun et nouveau. Principalement, il s'agit des communautés de logiciel Libre[(3)]. Le travail fourni par ce type de communauté est comparable à celui des professionnels en termes de qualité (Wikipédia par exemple). L'effort demandé à chacun est proportionnel à ses compétences compte tenu de la rigueur dans la qualité du produit final.

---

(1) M. GENSOLLEN, Les communautés en ligne : échanges de fichiers, partage d'expériences et participation visuelle, Editions Esprit, 2006.

(2) Les systèmes pair-à-pair permettent à plusieurs ordinateurs de communiquer via un réseau, en y partageant simplement des objets – des fichiers le plus souvent, mais également des flux multimédia continus (streaming), le calcul réparti, un service comme la téléphonie sur IP... .

(3) Un logiciel est libre si « *Premièrement, la liberté de copier un programme et de le redistribuer à vos voisins, qu'ils puissent ainsi l'utiliser aussi bien que vous. Deuxièmement, la liberté de modifier un programme, que vous puissiez le contrôler plutôt qu'il vous contrôle ; pour cela, le code doit vous être accessible.* », selon la définition qui en donne La Free Software Foundation (FSF) (littéralement « Fondation pour le logiciel libre »)

A partir de cette clarification, nous remarquons que chaque communauté dépend de l'objet qu'elle produit. La composante technologique (réseaux et plateformes d'échanges) est commune à toutes ces communautés et permet de faciliter le développement de leurs connaissances. Les mesures concernant l'effort et la contribution de chaque membre restent à préciser et se diffère d'une communauté à une autre. Par exemple, le partage d'une expérience d'un séjour dans un hôtel (communauté d'expérience) est beaucoup plus simple et moins onéreux que la participation au développement d'un nouveau logiciel libre (communauté d'épistémique).

Ces différences de comportement s'expliquent par certains éléments structurels qui existent et qui conditionne le comportement de chaque individu.

La contribution des individus à la production des connaissances sur Internet permet de créer de la valeur et de l'information disponible gratuitement à l'ensemble des utilisateurs. Les différentes applications Cloud Computing disponibles gratuitement sur Internet, permettent la génération de cette richesse. Par exemple : à titre d'exemple, Google met à disposition des utilisateurs des milliers de ressources gratuitement. Cependant, cette entreprise valorise ses activités via des ressources publicitaires en exploitant les données personnelles des individus collectées à travers leurs utilisations des services Google.

Ainsi, à travers leurs interactions quotidiennes sur Internet, les utilisateurs enrichissent la base des connaissances disponibles sur Internet mais également se construisent une identité qui les caractérise. Ainsi, les plateformes Internet, à partir de l'analyse des données collectées personnalisent les profils de chaque utilisateurs en utilisant des mécanismes Big data : analyse d'historiques des achats, rétentions des informations de connexion, analyses des historiques de recherches, analyse de l'expérience de l'utilisateur sur les réseaux sociaux, etc. Ainsi, ces utilisateurs construisent une identité numérique ou une cyber-identité, ainsi, ils deviennent des cyber-citoyens.

B. Identité numérique ou cyber-Identité

a) Contexte

Au moment d'introduction en bourse de Facebook, le nombre de ses utilisateurs dépassait les 900 millions, aujourd'hui ce chiffre est estimé à plus de 3 milliards de comptes pour une entreprise créée seulement il y a 10 ans. D'ailleurs, l'entreprise a célébré le 31 Août 2015, un milliard de connexions dans une seule journée. Selon Patrice Flichy[(1)], en 2009, un français sur cinq tenait un blog, ainsi, le citoyen français est un citoyen connecté.

Les outils numériques comme les blogs, les réseaux sociaux, *etc*., ont permis de démultiplier les espaces d'échanges entre individus et deviennent des espaces d'expression de soi. En effet, selon Luc Boltanski et Eve Chiappello[(2)], cette expression de soi est une tendance des sociétés « post-industrielles » née de la « critique artistique ». Cette dernière, elle-même issue des mouvements de 1968. Cette « critique artistique » a continué d'évoluer et avec l'avènement des technologies numériques.

Ainsi, les plateformes Internet ont donné la possibilité à chaque internaute de se construire une identité numérique et à chaque citoyen une cyber-identité fondée sur deux notions qui forment un couple : expressivité et intimité. Ainsi, l'identité numérique est composée de deux éléments principaux :

- *L'expressivité* : Il s'agit d'exprimer son opinion à travers des blogs politiques, des pages personnelles, des forums. Tous ces espaces appartiennent à un registre commun et véhicule un message précis destiné à un grand nombre de lecteurs. On parle donc de « *Logos* ».

- *L'intimité* : Il s'agit des opinions que l'on partage sur nos pages Facebook, et autres réseaux sociaux, des blogs intimes, *etc*. Toutes ces actions sont plutôt du ressort de l'intimité de l'individu qui cherche l'empathie de son entourage. On parle donc de la psyché.

Nous allons donc détailler ces deux notions.

---

(1) P. FLICHY, Le sacre de l'amateur Sociologie des passions ordinaires à l'ère numérique, Seuil, 2010.

(2) L. BOLTANSKI ET E. CHIAPPELLO, Le nouvel esprit du capitalisme, Gallimard, 1999

b) Expressivité

Les premiers outils de communication électronique limitent les échanges entre individus. En effet, depuis l'invention de téléphone en 1877, puis le courrier électronique et les premiers forums apparus avec l'Arpanet, ces outils ne permettaient pas des échanges riches mais seulement un envoie de texte sous forme de message court. Cette contrainte a fortement limité la richesse de l'expression des individus. Cependant, ces échanges limités réalisent ce que Judith Donath[(1)] appelle un « épouillage sociale » : échanger des banalités lors des rencontres afin de préserver la cohésion sociale d'un groupe ou d'une communauté.

Après le téléphone et le courrier électronique, des nouvelles formes d'échanges comme les réseaux sociaux, les blogs, *etc*., ont donné aux internautes d'autres moyens plus riches pour s'exprimer. Par conséquent, la notion s'est élargie considérablement d'abord à travers le discours (surtout le discours politique) puis via une expression culturelle des individus. En effet, certains internautes produisent des « biens culturels » sur leurs pages personnelles et les partages avec leur entourage. Cet « individualisme expressif » selon Laurence Allard et Frédéric Vanderbeghe[(2)] se construit grâce aux technologies de l'information et permet de révéler la personnalité de l'internaute aux autres. Par conséquent, le numérique a permis aux amateurs de produire et d'inventer leurs propres œuvres artistiques alors qu'ils avaient l'habitude de consommer les biens produits par les professionnels. Cette tendance a bien été appuyée par l'arrivée des plateformes Cloud de partage de vidéos comme Youtube et également la diffusion des réseaux sociaux comme Facebook ainsi que la multiplication des plateformes du financement participatif[(3)] comme *MyMajorCompany.fr*.

Les professionnels de la politique et les partis politiques ont pu diffuser largement leurs idées à travers des réseaux sociaux et plus précisément Twitter, qui connait une adoption significative par les personnalités politiques. Ainsi, le discours politique s'est diffusé grâce principalement à ce type de plateformes sociales. En effet, « Free of speech » ou la liberté de parole est souvent liée au discours politique à travers Internet. Cette liberté de parole est inscrite dans le premier amendement de la constitution des Etats-Unis, elle est devenue un droit institutionnel et a finalement envahi l'Internet. Selon Fabien Granjon[(4)], cette pratique a permet de révéler un certain nombre de fonctions comme la vulgarisation des connaissances ou la transmission du discours d'un expert ou simplement compléter un récit journalistique.

---

(1) J. DONATH, Signals in social supernets, journal of computer – Midiated Communication, 2007

(2) L. ALLARD ET F. VANDERBEGHE, Express yourself! Les pages perso, réseaux n° 1, 2003.

(3) Le financement participatif (en anglais crowdfunding) est une expression décrivant tous les outils et méthodes de transactions financières qui font appel à un grand nombre de personnes pour financer un projet à travers des plates-formes Internet. Ce financement participatif a été permis grâce à l'émergence d'Internet et des réseaux sociaux.

(4) F. GRANGON, Reconnaissance et usages d'internet, Les Presses des Mines, 2012.

D'après Dominique Cardon[(1)], l'expressivité des individus révélée par Internet a établi un nouvel espace d'échange intermédiaire entre l'espace public contrôlé principalement par des professionnels et l'espace privé des individus. Ce dernier permet une liberté de parole alors que dans l'espace public l'expression est contrôlée soit par les lois en vigueur soit par les « codes sociaux ».

c) Intimité

Les blogs et les réseaux sociaux ne permettent pas aux individus d'exprimer leurs talents artistiques en tant qu'amateurs mais ils exposent également leur intimité sur Internet. Les individus partagent souvent des évènements de familles, des évènements personnels : dates d'anniversaires, des examens, *etc*.

L'audience, ou les paramètres de confidentialités, est plus au moins maitrisé selon le niveau de sensibilisation de la personne, de ses connaissances technique mais également de la faisabilité de ce paramétrage dans l'outil utilisé (tous les outils ne permettent pas de gérer l'audience des publications). A titre d'exemple, Facebook favorise une audience « public » par défaut dans ses paramètres de confidentialité.

Cette intimité à travers les réseaux sociaux, plus au moins maitrisée selon les individus, révèle le niveau de sociabilité de chacun. En effet, selon Fabien Granjon et Julie Denouël[(2)], le fait que les individus s'affichent via les réseaux sociaux sur Internet permet de faire ce que l'on s'interdit dans le monde réel. Ils démontrent que via Internet, on se permet de montrer son corps, d'en jouer et d'afficher complètement son intimité physique. Une chose interdite dans le monde réel ou appartenant à la sphère strictement privée.

La motivation d'exposition de soi est évidente : s'exposer, présenter des éléments de son apparence et de sa personnalité, ce « auto-dévoilement » selon Serge Proulx[(3)], permet de créer une des interactions avec son « public » et susciter de l'empathie. Comme le souligne Olivier Voirol[(4)], plus les interactions sont nombreuses et riches plus l'on se construit une « psyché numérique ».

---

(1) D. CARDON, La démocratie Internet : Promesses et limites, Seuil, 2010.

(2) F. GRANGON, J. DENOUEL, « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », Sociologie 2010/1 (Vol. 1), p. 25-43.

(3) S. PROULX, L'irruption des médias sociaux: enjeux éthiques et politiques, Presses Universitaires du Québec, 2012.

(4) O. VOIROL, Les luttes pour la visibilité : Esquisse d'une problématique, La Découverte, 2005.

Ainsi, les différentes expressions de soi, expressivité ou intimité, à travers Internet, permettent à l'individu de construire sa propre cyber-expérience. Ainsi, « l'identité numérique peut être considérée comme une « représentation informatique » d'une entité »[(1)] qui divulgue, consciemment ou inconsciemment, des données personnelles parfois confidentielles, aux plateformes Internet. Ces derniers, exploitent ces données collectées à des fins commerciales : ciblage publicitaire, connaissance des tendances, achats manipulés, revente des données, etc. Cependant, les plateformes Internet ne sont pas les seuls à s'y intéresser. Ces données peuvent être également pour des fins de surveillance et de contrôle. En effet, le cyber-citoyen divulgue des informations en construisant sa propre cyber-identité. Certains, dont le Cyber-État, en profitent pour mettre en place des dispositifs de cybersurveillance comme nous l'avons vu précédemment.

C. Vie privée, Privacy et Sphère privée à l'ère du Cyber-État

a) Contexte

Dans cette partie, nous nous intéressons aux notions de la vie privée et de la protection des données personnelles telles qu'elles sont considérées dans le domaine de l'informatique. L'objectif n'est pas de décrire les textes règlementaires, mais d'identifier les éléments essentiels à considérer dans les solutions techniques du Cloud Computing et du Big data. Ainsi, les notions liées à la vie privée, ou à la sphère privée, sont fortement liées au terme « *privacy* ». Le terme *privacy* peut avoir plusieurs significations. Ainsi, il peut être utilisé pour signifier le droit à la vie privée (*right of privacy*) ou à la protection de la vie privée (*privacy protection*).

b) Vie privée

La mention du concept de vie privée est liée à un ensemble de problématiques liées à nos vies quotidiennes. Ainsi, la vie privée renvoie à la capacité de certains groupes ou individus à s'isoler afin de se recentrer sur leurs vies privées et de protéger leurs intérêts de la vie publique.

La notion de surveillance d'un individu, de sa cybersurveillance, l'enregistrement ou le traitement d'informations le concernant, le fait d'entrer en communication avec lui sur la base des résultats d'un traitement Big data sont autant d'actions en lien étroit avec la notion de vie privée ou de sphère privée. Le concept semble donc composite et par conséquent difficile à cerner. A cela s'ajoute le concept du respect de la vie privée, qui est aussi un concept difficile à saisir parce que sa signification dépend du contexte, y compris du lieu géographique.

Ainsi, comme nous allons le voir dans la suite, le respect de la vie privée est identifié comme un droit fondamental dans la majorité des traités internationaux, dans les accords sur les droits de l'homme et dans une majorité des constitutions de la plupart des pays.

[(1)] M. LAURENT ET S. BOUZEFRANE, La gestion des identités numériques, Londres, ISTE, 2015

c) Privacy

Concernant le mot *privacy,* Alan Westin définit ce terme en adoptant un point de vue de type juridique, confondant en un seul et même mot l'objet et le droit à l'objet :

> «*Right of individuals to determine for themselves when, how and to what extent information about them is communicated to other.* »[(1)].
>
> En français:
> « *Le droit des individus à déterminer pour eux quand, comment et quelles informations les concernant doivent être communiquées aux autres* »

Pour Günter Müller, la notion de la *privacy* renvoie vers :

> *« Possibility to control the distribution and use of personal data* »[(2)].
>
> En français:
>
> *« La possibilité de contrôler la distribution et l'utilisation des données personnelles* ».

Par conséquent, nous constatons que les deux définitions semblent limiter la notion de vie privée à une diffusion maîtrisée d'informations.

Ainsi, Sara Baase[(3)] propose une acception légèrement différente et sans doute plus «significative », suivant laquelle le mot *privacy* peut signifier indifféremment :

- L'absence d'intrusion ;
- Le contrôle des informations personnelles;
- L'absence de surveillance.

Cependant, ces définitions de la notion de vie privée peuvent également paraître «*peu innocentes* » dans le cadre d'un Cyber-État à cause de l'intrusion des notions comme la cybersurveillance.

d) Le concept de « Privacy by design »

La notion « Privacy by design » est une notion récente qui est apparue à la fin des années 1990 sous l'impulsion de la Commissaire canadien à l'information et à la protection de la vie privée de l'Ontario Ann Cavoukian[(4)]. Cette notion vient remédier à une problématique qui consiste à dire que le cadre légal ne peut intervenir que postérieurement à une atteinte à aux données personnelles ainsi au respect de sa vie privée. L'action se fait donc à posteriori de l'incident.

L'objectif de la nouvelle approche de « Privacy By Design » est d'intégrer les principes du respect de la vie privée et précisément des données personnelles directement dans la conception d'un système informatique. Elle vise à agir en amont afin d'éviter tout abus et atteinte à la vie privée des utilisateurs de ces mêmes systèmes informatiques en proposant aux utilisateurs plusieurs démarches par exemple :

- Démarches préventives des abus potentiels suite à l'utilisation d'un système informatiques ;
- Démarches de vulgarisation des modalités de fonctionnement de ce même système informatique ;
- Démarche d'orientation des utilisateurs vers le meilleur choix possible pour protéger leurs données personnelles ;

---

(1) A. WESTIN, Privacy and freedom, New York. USA. 1967. p. 54.

(2) G. MULLER, Introduction of privacy and security in highly dynamic systems, Communications of the ACM, 2006, P. 42.

(3) S. BAASE, A Gift of Fire: Social, Legal, and Ethical Issues in Computing, Prenctice-Hall, 2003.

(4) A. CAVOUKIAN, Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, 2009

La résolution proposée par A. Cavoukian, qui consiste à dire que « *la protection intégrée de la vie privée [constitue] un concept global pouvant s'appliquer à l'ensemble des activités d'une organisation de bout en bout, y compris à la technologie de l'information, aux pratiques administratives, aux procédés, à la conception matérielle et aux réseaux* », a été adoptée durant la 32e Conférence internationale des Commissaires à la protection des données et de la vie privée[(1)] qui a eu lieu en Octobre 2010.

Cette approche d'action en amont pour prévenir tout abus lié aux données personnelles a été prise au sérieux par le législateur européen mais aussi les américains et précisément Federal Trade Commission (FTC) [(2)], les deux parties se sont intéressées à cette résolution qui consiste à « *favoriser l'intégration des principes fondamentaux… dans le libellé des politiques et textes de loi sur la protection de la vie privée dans leur territoire de compétence* ».

Le concept de « Privacy By Design » s'articule principalement autour de 7 principes généraux qui «*décrivent les mesures proactives à prendre pour faire de la protection [des données personnelles] le mode implicite de fonctionnement de toutes les organisations, tout en assurant une fonctionnalité intégrale* ». Ces 7 principes fondamentaux sont donc :

- Prendre des mesures proactives et non réactives ; des mesures préventives et non correctives ;
- Assurer la protection implicite de la vie privée ;
- Intégrer la protection de la vie privée dans la conception ;
- Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle ;
- Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements ;
- Assurer la visibilité et la transparence ;

---

(1) 32e Conférence internationale des Commissaires à la protection des données et de la vie privée, Résolution sur la protection intégrée de la vie privée, du 27 au 29 oct. 2010, Jérusalem, Israël, https://www.ipc.on.ca/site_documents/pbd-resolution-f.pdf

(2) Aux États-Unis, la Federal Trade Commission (FTC) a notamment recommandé dans son rapport « Protecting consumer privacy in an Era of rapid Change » de mars 2012 que les entreprises adoptent une approche Privacy by design.

e) Sphère privée

Les diverses définitions vues précédemment renvoient à des concepts de la vie courante se réduisent à un problème de contrôle de l'information. Ainsi un nouveau concept apparait. Il s'agit du concept de « sphère privée »[(1)].

En effet, la sphère privée d'un individu est l'ensemble des informations se rapportant à lui-même, qu'il considère comme sensibles et donc dignes d'être protégées. Cette sphère est personnelle (l'individu est le propriétaire des informations qu'elle contient), personnalisable (l'individu décide des informations qu'elle contient), dynamique (les informations peuvent y être ajoutées ou en être retirées) et dépendante du contexte (les informations qu'elle contient peuvent, en nature et en nombre, dépendre du temps, des activités de l'individu ou d'autres paramètres). La sphère privée encapsule donc toutes les informations, explicitement représentées ou non, qui nous concernent et que nous souhaitons protéger pour quelque motif que ce soit. Ainsi, comme c'est le cas pour le respect de la vie privée, le respect de la sphère privée est également identifié comme un droit fondamental qui doit être préservé par les traités nationaux et internationaux.

D. La problématique de protection des données à l'ère du Cyber-État

La protection des données personnelles consiste en l'ensemble des mesures visant à assurer le respect du droit à une vie privée. Cependant, ces mesures sont limitées aux données de la sphère privée d'un utilisateur représentées sous forme numérique et mises en jeu dans le cadre d'un Cyber-État.

Ainsi, l'étude des textes juridiques et réglementaires fait ressortir six thèmes principaux, suivant lesquels s'alignent les diverses réglementations. Ces thèmes sont :

- L'information de l'utilisateur ;
- Le consentement de l'utilisateur ;
- Le droit d'accès et de modification pour l'utilisateur ;
- Le principe de justification de la collecte et du traitement ;
- La conservation des données et leur transmission à des tiers.

[(1)] L. CREPIN, L. VERCOUTER, F. JACQUENET, Y. DEMAZEAU et O. BOISSIER, « Hippocratic multi-agent systems», The International Conference on Enterprise Information Systems (ICEIS'08). Pages 301–307, 2008.

En se restreignant au monde numérique, on reconnaît que l'on ignore délibérément tous les éléments de la sphère privée qui ne sont pas directement représentables dans un fichier informatique donc ne font pas partie du cadre de réglementation d'un Cyber-État. Cependant, la frontière reste floue entre les deux mondes et a tendance à se rapprocher avec les évolutions technologiques qui ne cessent de s'introduire de plus en plus dans nos vies quotidiennes, et de transformer le citoyen à un cyber-citoyen hyper connecté.

Ainsi, la diffusion des plateformes Internet est en grande partie responsable de l'évolution des inquiétudes du grand public quant à la protection de sa vie privée en général, et de ses données personnelles, parfois sensibles, en particulier comme les données de santé ou informations bancaires. A cela s'ajoute, la nature du Cyber-État, son caractère dématérialisé, qui amplifie des programmes de cybersurveillance des individus à leurs insu. Divers domaines de la vie privée peuvent donc servir comme cas d'utilisation dans lequel se posent des problématiques de protection de vie privée et toute interaction de cyber-citoyen avec Internet laisse des traces qui pourront être utilisé par à des fins commerciales ou à des fins de sécurités à travers une cybersurveillance, sauf, si des réglementations sont mises en place afin de protéger le cyber-citoyen d'un abus du pouvoir par le Cyber-État ou d'excès commercial des plateformes Cloud.

Dans la prochaine partie, nous aborderons les principales réglementations qui vont dans ce sens en nous basant sur différents travaux de la chaire « Valeurs et politiques des informations personnelles » dont nous faisons partie. Par la suite, nous présenterons les deux organismes chargés de la protection des données personnelles en France (la CNIL) et au Maroc (CNDP).

E. Les principaux textes réglementaires de protection des données personnelles

a) Contexte

Les textes de lois et les différentes directives que nous allons présenter dans cette partie déterminent dans leur ensemble, ce qui peut ou ne peut pas être fait des données informatiques susceptibles d'être rattachées à un individu particulier.

Ces textes réglementaires que nous allons aborder réduisent la sphère privée d'un individu à sa partie observable par un système électronique ou informatique, aux informations qui peuvent être extraites, représentées et reliées entre elles. Ces textes constituent donc une projection du principe général exprimé par le Code Civil sur le domaine de l'informatique et des télécommunications.

Ainsi, la réglementation de protection des données personnelles concernent l'ensemble des informations fournies par l'utilisateur, consciemment ou inconsciemment, à travers son usage de des outils numériques : Téléphones, Internet, Objets connectés, *etc*.

b) La loi française 78-17 « Informatique et Libertés »

La spécificité des risques induits par les traitements automatisés des informations (et notamment ceux mis en œuvre par les administrations publiques), a motivé la création d'une nouvelle loi en 1978. Ainsi, La France est alors le premier pays européen à inclure dans son droit national des dispositions spécifiques concernant les traitements informatiques de données personnelles.

La loi 78-17 du 6 janvier 1978, « relative à l'informatique, aux fichiers et aux libertés » (dite loi « Informatique et Libertés ») parle de traitements automatisés sur des données nominatives. Ce texte pose des principes qui sont depuis rentrés dans la culture française, de par les mentions légales apparaissant systématiquement dans les formulaires de collecte de données.

Les données nominatives dans ce texte légal sont définies comme celles pouvant être rattachées à une personne, de manière directe ou indirecte. Cette précision permet d'englober les données pouvant être liées à une personne après recoupement avec d'autres informations. Le responsable d'un traitement automatisé ou d'une base de données contenant ce type d'informations ne les possède pas, mais est responsable de leur sécurité.

Le texte introduit l'obligation fondamentale d'informer l'intéressé sur divers points concernant le traitement et de recueillir son consentement (sauf dans certains cas particuliers prévus par la loi, comme par exemple l'accomplissement d'une mission de service public). L'intéressé jouit également d'un droit d'accès et de rectification des données collectées, exerçable auprès du responsable du traitement.

c) La loi marocaine 09-08 (BO n°5714 du 05-03-2009)

Dans le cadre de leurs missions sur le territoire marocain, les organismes publiques et privées (marocains ou étrangers) sont amenés à effectuer des traitements de données, en vue d'assurer un ensemble d'opérations tels la paie, la facturation, la vidéosurveillance, l'enregistrement des visiteurs, le contrôle d'accès aux locaux, les campagnes de marketing direct, la tenue de sites marchands, la journalisation des connexions Internet, etc.

La loi 08-09 définit les données à caractère personnel comme étant toute information, de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable dénommée par la loi «personne concernée». Elle s'applique aux données à caractère personnel, automatisé en tout ou en partie mais également aux données traitées permettant d'identifier une personne dans des fichiers manuels.

> **[Art. 1]**
> *« L'informatique est au service du citoyen et évolue dans le cadre de la coopération internationale. Elle ne doit pas porter atteinte à l'identité, aux droits et aux libertés collectives ou individuelles de l'Homme. Elle ne doit pas constituer un moyen de divulguer des secrets de la vie privée des citoyens. Pour l'application de la présente loi, on entend par:*
>
> *1-« données à caractère personnel»: toute information, de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant -2-une personne physique identifiée ou identifiable, dénommée ci-après «personne concernée». Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;*
>
> *2-«traitement de données à caractère personnel» («traitement»): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction;*
>
> *3-«données sensibles» : données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale de la personne concernée ou qui sont relatives à sa santé y compris ses données génétiques ;»*

4-«fichier de données à caractère personnel» («fichier») : tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographiques, tels que les archives, les banques de données, les fichiers de recensement;

Les traitements des données personnelles sont, en général, indispensables aux organismes pour répondre à des exigences administratives, organisationnelles ou commerciales. Mais ils risquent de porter atteinte à la vie privée et aux droits des personnes concernées. L'enjeu donc est de trouver le juste équilibre entre le besoin d'utiliser ces données par les organismes et le respect des droits des personnes concernées. C'est à cette fin que la loi 09-08 a été adoptée et que la Commission Nationale de contrôle de la protection des Données à Caractère Personnel (C.N.D.P) a été créée.

5-« responsable du traitement» : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires, le responsable du traitement doit être indiqué dans la loi d'organisation et de fonctionnement ou dans le statut de l'entité légalement ou statutairement compétente pour traiter les données à caractère personnel en cause;

6-«sous-traitant»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

7-«tiers»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données;

8-«destinataire»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers.

Ainsi, tous les traitements dont les responsables ou les moyens de traitement sont situés sur le territoire marocain, qu'ils soient propriété d'un organisme marocain ou d'un donneur d'ordre étranger (sous-traitance, délocalisation, etc.), sont soumis à la loi 09-08 du 18 février 2009 (BO n°5714 du 05-03-2009) ainsi qu'à l'autorité de la Commission Nationale de Protection des Données Personnelles (CNDP) que nous aborderons dans la suite de cette section.

d) Lignes directrices de l'OCDE

L'OCDE est une organisation constituée de 30 membres qui partagent le même engagement vis-à-vis une société démocratique. En effet, L'OCDE est la première organisation internationale à avoir essayé d'unifier les initiatives relatives à la protection des données personnelles. En 1980, elle a publié les « *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel* ».

Ainsi, nous pouvons regrouper l'ensemble des lignes directrices de l'OCDE par les huit principes suivants que nous retrouvons dans les différentes initiatives de l'organisation:

[Action 1 : Limitation en matière de collecte]
«*Il convient de fixer des limites sur la collecte de données à caractère personnel et toute information de ce type doive être obtenue par des moyens licites et loyaux et ceci après avoir informé la personne concernée ou avec son consentement*».

[Action 2 : Qualité des données]
« *Les données à caractère personnel doivent être congruents aux finalités en vue desquelles elles seront utilisées et, dans la mesure où ces finalités l'exigent, elles doivent être exactes, complètes et tenues à jour* » ;

[Action 3 : Spécification des finalités]
« *Les finalités en vue desquelles les données à caractère personnel sont collectées doivent être déterminées au plus tard au moment de la collecte. Elles ne doivent être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne sont pas incompatibles avec les précédentes et comme sont spécifiés à chaque occasion de changement de finalité*» ;

[Action 4 : Limitation de l'utilisation]
« *Les données à caractère personnel ne doivent pas être divulguées, ni fournies, ni utilisées à d'autres fins que celles spécifiées conformément au principe de la spécification des finalités*»

***[Action 5 : Garanties de sécurité*]**
« *Il convient de protéger les données à caractère personnel, moyennant des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés*» ;

[Action 6 : Transparence]

« *Il convient d'assurer, de façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données à caractère personnel. Il doit être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données à caractère personnel, et les finalités principales de leur utilisation, ainsi que l'identité du dépositaire du fichier et le siège habituel de ses activités* » ;

[Action 7 : Participation individuelle]

« *Toute personne doit avoir le droit d'obtenir du dépositaire du fichier, ou par d'autres voies, confirmation du fait que le dépositaire du fichier détient ou pas des données la concernant* » ;

[Action 8 : Responsabilité]

« *Tout dépositaire de fichier doit être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus*. »

Les lignes directrices de l'OCDE représentent le consensus des pays membres concernant la collecte et de la gestion de l'information personnelle. Les principes du respect de la vie privée définis sont caractérisés par leur clarté et leur flexibilité pour s'adapter aux évolutions technologiques mais également à une flexibilité de prendre en compte certaines spécifiés au niveau national : Par exemple la complémentarité de ces lignes avec les dispositifs de la CNIL en France.

e) Directives du Conseil de l'Europe

Le 28 janvier 1981 à Strasbourg, le Conseil de l'Europe a adopté la «Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » connues sous le nom de « convention 108 du Conseil de l'Europe ».

Cette convention est le premier instrument international obligatoire qui protège l'individu contre des abus d'exploitation de ses données à caractère personnel.

En 1995, l'Union Européenne a adopté la directive (95/46EC) sur la « protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » connue sous le nom de « directive de protection des données d'UE». Cette proposition était la réponse à la perception des insuffisances des recommandations concernant le respect de la vie privée de l'OCDE et la convention 108 du Conseil de l'Europe.

Ainsi, selon les termes des directives d'UE, chaque pays de l'UE doit avoir un commissaire ou une agence de protection des données qui impose les règles, c'est le cas de la Commission Nationale d'Informatique et Liberté (CNIL). Cependant, en adoptons ce type de directive, l'UE s'attendait à ce que les pays avec lesquels l'Europe fait des affaires, fournissent un niveau de régulation identique. Nous pensons spécialement aux États-Unis.

f) La directive européenne 95/46/CE

La directive européenne 95/46/CE « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* » est le premier et le principal texte réglementaire de l'Union européenne en matière de protection de la vie privée. Dans ce texte, le vocabulaire change par rapport à la loi 78-17. Ainsi, un changement majeur concerne l'utilisation de données personnelles au lieu de données nominatives. Ce nouveau terme apparaitra par la suite dans les textes réglementaires français.

Dans ce cadre, il est interdit de collecter des données à l'insu de l'utilisateur ou contre son gré. De plus, il est spécifié que les données collectées doivent être «adéquates, pertinentes et non excessives au regard » de « finalités déterminées, explicites et légitimes».

La directive introduit également un lien entre les données collectées et le but du traitement. Il est précisé qu'il est interdit de collecter des données superflues, non nécessaires, non directement liées au but poursuivi. Cette directive introduit également la notion de collecte minimale de données, qui sera par la suite interprété comme un concept de transmission minimale de données, préservant le caractère privé de ses informations.

Ces aspects de la protection de la vie privée sont également désignés dans la littérature sous les termes de principe de proportionnalité et de principe de finalité. Le texte introduit des dispositions particulières pour interdire les traitements portant sur des données très

sensibles, comme les convictions religieuses, l'orientation sexuelle ou les informations relatives à la santé tout en réaffirmant des principes comme le renforcement de la protection vis-à-vis de la diffusion des données, et en imposant une nouvelle phase d'information de l'intéressé lorsque ses informations sont utilisées par un tiers.

Les transferts de données à destination de pays tiers sont également réglementés et limités aux pays pouvant justifier d'un « niveau de protection adéquat ».

Concernant le contrôle de l'application des diverses dispositions, la directive impose à chaque pays membre la création d'une autorité de contrôle nationale (la CNIL en est le représentant français), et leur regroupement en un « groupe de protection des personnes à l'égard du traitement des données à caractères personnel ». Cette organisation européenne est communément appelée « groupe de l'article 29 » ou plus couramment encore G29 dont la commission marocaine du contrôle des données personnelle (CNDP) fait partie.

g) La directive européenne 02/58/CE

La directive européenne 02/58/CE *«concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques»* est un exemple d'application sectorielle des principes de la directive de 1995. Elle définit des dispositions techniques de protection de la vie privée spécifiques au secteur des télécommunications. Elle reprend chacun des principes de base, pour les transcrire dans ce cas d'application particulière.

Un des intérêts de cette directive est qu'elle traite des transmissions électroniques non sollicitées (spam en anglais), en établissant clairement une priorité de l'opt-in qui signifie que si l'intéressé n'a pas explicitement donné son consentement pour être contacté par une société particulière, alors cette société ne peut utiliser ses informations personnelles pour lui faire une offre commerciale. Néanmoins, si l'intéressé a déjà eu recours aux services d'une société, la directive considère qu'il est légitime que celle-ci le recontacte pour lui proposer des services semblables.

Ce texte réaffirme également le principe de la collecte minimale d'informations introduit par la directive de 1995. Ainsi, l'article 14-3 de la directive stipule que :

> *« Des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel ».*

La législation européenne garantit donc théoriquement les utilisateurs contre la construction de matériels électroniques ou informatiques trop intrusifs, ou de manière générale présentant un risque pour leur vie privée.

h) Le nouveau règlement européen de protection des données personnelles

Depuis le 14 Avril 2016 et après des années de négociation entre les différents acteurs, le parlement européen a adopté un règlement majeur en matière de régulation des données personnelles. Ce nouveau règlement vise à renforcer la maitrise des traitements des données personnelles par les individus, entreprises et les autorités du contrôle, tout en renforçant le cadre juridique associé. Ce nouveau texte n'est pas une directive européenne mais un texte applicable directement au niveau européen sans nécessiter de transposition dans les différents États-membres. Ainsi, ce même texte s'appliquera dans toute l'Union sans exception.

Avec ce texte, le citoyen européen voit ses droits existants renforcés au niveau du traitement mais aussi au niveau du contrôle, qui lui devient accessible dans un format clair et compréhensible en introduisant par exemple le principe de portabilité qui permet à unl individu de demander l'accès à ses informations et les porter vers une nouvelle plateforme. Pour les entreprises, ce nouveau règlement européen introduit une simplification des formalités administrative à travers la notion de l'interlocuteur unique pour toutes les démarches administratives. Ce nouveau règlement introduit également des nouveaux dispositifs liés à la certification des entreprises en matière de protection des données personnelles mais au aussi en matière du respect d'un code de bonne conduite en matière du traitement des données personnelles. Les autorités du contrôle, quant à elles, se voient attribuer des nouvelles compétences en matière du contrôle des établissements installés sur le territoire européen. Les pouvoirs de répression ont été également renforcés et les autorités peuvent sanctionner administrativement ou financièrement toute entreprise faisant l'objet d'une fraction de ce nouveau règlement. La collaboration entre les différentes autorités du contrôle européen est également prévue. Ces dernières peuvent prononcer des décisions collectives pour un cas similaire dans différents pays. Ce mécanisme va renforcer l'intégration européenne en matière de protection des données personnelles.

C'est dans cette intégration européenne que le nouvel organisme appelé « le Comité Européen de la Protection des Données (CEPD) » sera mis en place. Ce dernier aura pour mission de coordonner les différentes entités du contrôle et également d'arbitrer les différents entre ces mêmes entités. Ce nouvel organisme remplacera à terme le « G29 » et viendra développer la doctrine européenne en matière de protection des données personnelles. Ce nouveau dispositif européen entrera en vigueur dès Avril 2018, l'ensemble des autorités de G29 travaillent actuellement dans le cadre d'un plan d'action pour préparer le terrain à l'application des dispositifs annoncés. Les principaux objectifs fixés pour les deux à venir sont :

- Préparer la mise en place du Comité européen de la protection des données (CEPD), qui remplacera le G29 en 2018 ;

- Préparer la mise en place du guichet unique et le mécanisme coopération et de cohérence entre les autorités ;

- Proposer des lignes directrices ou des bonnes pratiques aux professionnels pour les 4 sujets prioritaires identifiés: le droit à la portabilité, la certification, le délégué à la protection des données (DPO), les traitements à risque ;

- Promouvoir et diffuser le règlement afin que l'ensemble des acteurs se l'approprie.

Comme le détaille la CNIL, les différents dispositifs apportés par ce nouveau règlement apportent principalement les éléments suivants :

- Un cadre juridique unifié pour l'ensemble de l'UE : Comme nous l'avons signalé plus haut, ce texte n'est pas une directement mais un règlement applicable sur l'ensemble de l'Union sans exception. Ainsi, il permet de :
    - Étendre les champs d'application qui permet d'élargir les critères de ciblage pour les responsables de traitement ou les sous-traitants établies établi sur le territoire de l'Union européenne ou mettent en œuvre des traitements visant à fournir des biens et des services aux résidents européens. Ces derniers se voient imposées les mêmes obligations initialement prévues pour le responsable du traitement.
    - Un guichet unique : le « one stop shop » qui permet aux entreprises, ayant des traitements transnationaux, d'avoir une autorité du contrôle comme interlocutrice unique. Cette dernière est principalement établie dans le même État membre.
    - Une intégration renforcée entre les différentes autorités nationales pour gérer les traitements transnationaux touchant les citoyens de plusieurs États-membres. Cette intégration permet de fournir une réponse unique et unifiée et ainsi arbitrer des éventuels différends entre les différents États.
- Un renforcement des droits des personnes : Le nouveau règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci. Il apporte principalement les dispositions suivantes :
    - La mise en place d'un mécanisme d'un consentement renforcé et transparent à travers une information claire et définie. Ainsi les utilisateurs sont informés de l'exploitation de ces données et doivent acceptés
    - La mise en place d'un droit à la portabilité des données qui permet aux utilisateurs de récupérer leurs données sous un format facilement exploitable
    - La mise en place des dispositifs clairs et simplifiés pour la gestion des données des enfants de moins de 16 ans. L'objectif est de permettre aux enfants de comprendre d'une façon simple les conditions d'utilisations de leurs données personnelles

    - La mise en place d'un droit à réparation des dommages matériel ou moral pour toute personne ayant subi un dommage matériel ou moral du fait d'une violation de ce nouveau règlement de protection des données personnelles.
    - La mise en place du principe des recours collectifs qui permettront à un groupe d'individus de faire une action collective en matière des données personnelles à l'instar des associations de protection des consommateurs.
- La mise en place des mécanismes de conformité basée sur une logique de conformité dont les acteurs sont responsables contrairement à la directive européenne de 1995 qui repose sur la conformité préalable de type déclaration ou autorisation. Ce dispositif consiste principalement en :
    - La mise en place d'une protection des données dès la conception et par défaut (privacy by design) qi permet de mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »)
    - La mise en place d'un allégement des formalités administratives qui vont permettre de démontrer facilement la conformité des mesures de protections des données personnelles : Le principe de l'Accountability. Les outils permettant la vérification de cette conformité peuvent être sous forme d'un registre à maintenir ou des systèmes de certification et de bonne conduite.
    - La mise en place des mécanismes de responsabilisation des acteurs qui va permettre de supprimer les processus déclaratifs dès que le traitement des données ne constitue pas un risque pour la protection des données des utilisateurs.
- Le nouvel règlement européen a également renforcé le cadre de transfert des données personnelles hors de l'Union Européenne en mettant en place des outils assurant la protection des données transférées. Ces données resteront soumises au droit de l'Union non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur. Parmi ces nouveaux outils mis en place :
    - Pour les sous-traitants : la possibilité de mettre en place des règles d'entreprises contraignantes ;
    - Pour les autorités publiques : le recours à des accords contraignants ;
    - Pour les responsables de traitement et les sous-traitants : l'adhésion à des codes de conduite ou à un mécanisme de certification. Ces deux outils doivent contenir des engagements contraignants ;

F. France : Commission Nationale d'Informatique et des Libertés (CNIL)

1) Contexte

La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que les technologies de l'information soient au service du citoyen et qu'elles ne portent atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi no 78-17 du 6 janvier 1978 modifiée le 6 août 2004.

En effet, en adoptant le 6 janvier 1978, une loi relative à l'informatique, aux fichiers et aux libertés, la France s'équipe des outils nécessaires pour protéger les données personnelles face aux dangers que leur mise sur Internet fait courir à la vie privée au cyber-citoyens à l'ère de diffusion des technologies de Cloud Computing et de Big data. Le dispositif repose sur le fait que la responsabilité principale de la protection revient cependant à une autorité administrative indépendante la CNIL. Elle doit veiller au respect d'un certain nombre de principes, de finalité, de transparence. Elle doit s'assurer également que la limitation dans la durée de conservation des informations est respectée. Plus généralement, son statut et ses prérogatives doivent lui permettre d'éviter que l'informatisation porte atteinte à la vie privée des personnes et des usagers.

Ainsi, après plusieurs années de sa mise en place, il serait pertinent d'analyser les grands traits de régulation que la CNIL a réussi à établir et les difficultés qu'elle a rencontrées dans l'accomplissement de cette tâche. En effet, selon Armand Mattelart[(1)], souligne que l'évaluation des travaux de la CNIL est utile dans ce contexte où le respect des libertés et des droits fondamentaux sont remis en cause par l'évolution des techniques et par le contexte politique. De ce fait, dans une dictature, l'ensemble des informations personnelles des citoyens deviennent des armes pouvant être utilisés par les pouvoir. Ainsi, la surveillance de l'individu par l'information a pris une importance croissante sans que, ces mêmes individus, en prenne conscience[(2)]. Ainsi, cette surveillance peut même constituer un des traits essentiels de notre société définie comme une société de contrôle[(3)] comme le souligne James Rule « *que les quatre dernières décennies ont valu aux démocraties de ce monde, de plus en plus de législation et d'institutions vouées à la protection de la vie privée, mais de moins en moins de vie privée* »[(4)].

---

(1) A. MATTELART, La Globalisation de la surveillance, Paris, La Découverte, 2007.

(2) Voir principalement: 1) C. TAYLOR, The Malaise of Modernity, Anansi, 1991. 2) A. GIDDENS, La Constitution de la société, Paris, PUF, 1987 et 3) G. DELEUZE, « Post-scriptum sur les sociétés de contrôle », Pourparlers, Paris, Éd. de Minuit, 1990.

(3) A. VITALIS, «Informatique et libertés » : une histoire de trente ans, C.N.R.S. Editions, 2009.

(4) J. RULE, « Deux parcours divergents : les climats politiques et l'accessibilité croissante des renseignements personnels », Actes du 14e colloque du Creis, Paris, juin 2007.

2) La loi Informatique et libertés

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés (LIL) et réglemente aujourd'hui les pratiques liées aux traitements des données par des outils informatique. Elle est découpée en treize parties, dont seules les trois premières (Principes et définitions, Conditions de licéité des traitements de données à caractère personnel, La commission nationale de l'informatique et des libertés) concernent directement les particuliers. Ainsi, les articles abordant explicitement le traitement des données à caractère personnel sont les suivants :

[Article 1]

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.»

[Article 2]

« [...] Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

« […]Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

« […] Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés. La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement. »

[Article 3]

« Toute personne habilitée à recevoir communication de ces données »

[Article 6]

« Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

- *Les données sont collectées et traitées de manière loyale et licite ;*
- *Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;*
- *Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;*
- *Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées;*
- *Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »*

[Article 7]

« *Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :*

- *Le respect d'une obligation légale incombant au responsable du traitement ;*
- *La sauvegarde de la vie de la personne concernée ;*
- *L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;*
- *L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;*
- *La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée »*

3) Les missions principales de la CNIL

La loi Informatique et Libertés (LIL) a précisé la nature des missions confiées à la CNIL. Elles peuvent être résumées en 6 missions principales selon ***l'article 11*** de la loi LIL. Ainsi, nous pouvons reformuler ces missions comme suit :

- **Informer** :
  La CNIL est investie d'une mission générale d'information des personnes sur leurs droits et leurs obligations. Elle aide les citoyens dans l'exercice de leurs droits ;

- **Réguler** :
  La CNIL régule et recense les fichiers, autorise les traitements les plus sensibles avant leur mise en place. L'avis de la CNIL doit d'ailleurs être sollicité avant toute transmission au Parlement d'un projet de loi relatif à la protection des données personnelles ; il doit aussi être sollicité par le Gouvernement avant d'autoriser les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique ;

- **Protéger** :
  La CNIL doit veiller à ce que les citoyens soient informés des données contenues dans les traitements les concernant et qu'ils puissent y accéder facilement. Elle reçoit et instruit les plaintes des personnes qui rencontrent des difficultés à exercer leurs droits ;

- **Contrôler** :
  La CNIL vérifie que la loi est respectée en contrôlant les traitements informatiques. Elle peut de sa propre initiative se rendre dans tout local professionnel et vérifier sur place et sur pièce les fichiers. La Commission use de ses pouvoirs d'investigation pour instruire les plaintes et disposer d'une meilleure connaissance de certains fichiers ;

- **Sanctionner** :
  Lorsqu'elle constate un manquement à la loi, la CNIL peut, après avoir mis en demeure les intéressés de mettre fin à ce manquement, prononcer diverses;

- **Anticiper** :
  La CNIL doit s'attacher à comprendre et anticiper les développements des technologies de l'information afin d'être en mesure d'apprécier les conséquences qui en résultent pour l'exercice des droits et libertés. Elle propose au Gouvernement les mesures législatives ou réglementaires de nature à adapter la protection des libertés et de la vie privée à l'évolution des techniques.

4) La CNIL et la cybersurveillance

i. Position de la CNIL par rapport à loi relative au renseignement

Selon son avis[(1)] rendu officiel le 19 Mars concernant la loi relative au renseignement, la CNIL souligne certaines réserves vis-à-vis certaines dispositions clés du projet de loi qui vise à généralisé une surveillance (ou une cybersurveillance) «officialisée».

Ainsi, selon l'avis de la CNIL, ces outils de surveillance opèrent un changement de paradigme dans les techniques de renseignement :

> « *un changement aux conséquences particulièrement graves sur la protection de la vie privée et des données personnelles […] Il ne s'agit plus seulement d'accéder aux données utiles concernant une personne identifiée, mais de permettre de collecter de manière indifférenciée, un volume important de données qui peuvent être relatives à des personnes tout à fait étrangères à la mission de renseignement*.».

D'après la CNIL, trois outils sont particulièrement inquiétants dans le cadre de l'adoption de cette loi relative au renseignement :

- *Le premier outil concerne les « métadonnées »*. Ainsi, cet outil permet la captation des données de connexion (soit les métadonnées) en temps réel et directement sur les équipements des opérateurs télécoms. L'objectif est de pouvoir détecter des actes potentiels du terrorisme liés à des suspects déjà identifiés. Le projet de loi prévoyant que les services puissent à ce titre prélever « *la totalité des informations et documents* ». Ainsi, dans ses préconisations, la CNIL souhaite que le périmètre concernait par cette pratique soit clarifié ainsi que la nature et le type des données qui peuvent être collectées. Ainsi, on peut lire dans cet avis de la CNIL :

  > « *Les garanties prévues pour préserver les droits et libertés ne sont pas suffisantes pour justifier une telle ingérence* » ;

- *Le deuxième outil concerne le système de détection automatique d'activités de nature terroriste*. En effet, le projet de loi officialise également la création d'un système de détection automatique d'activités de nature terroriste sur la base de données informatiques « anonymes ». La CNIL souligne que l'anonymat de ces données est tout relatif dans la mesure où il peut être levé « en cas de caractérisation de menace terroriste » ;

---

(1) L'avis complet disponible sur le site institutionnel de la CNIL via l'URL (dernière consultation 21/09/2015): http://www.cnil.fr/nc/linstitution/actualite/article/article/publication-de-lavis-sur-le-projet-de-loi-relatif-au-renseignement/

- *Le troisième outil concerne les appareils « IMSI catchers».* En effet, les « IMSI catchers » sont des appareils qui imitent les antennes-relais de téléphonie mobile afin de capter les communications d'un suspect. Selon la CNIL, ce dispositif très intrusif devrait être soumis au même système de contrôle que les autres techniques de surveillance, alors que le projet de loi n'en soumet l'utilisation qu'à des procédures très légères. *« Un tel dispositif permettra de collecter de manière systématique et automatique des données relatives à des personnes pouvant n'avoir aucun lien ou un lien purement géographique avec l'individu effectivement surveillé ».*

ii. Position de la CNIL par rapport à la loi antiterroriste

La CNIL a émet des réserves sur l'adoption de la loi antiterroriste. En effet, dans un avis rendu officiel, la CNIL considère que :

> « *les dispositifs prévus par le projet de loi ne devraient être envisagés qu'en tant que mesures exceptionnelles […] être assortis de garanties et de contrôles particulièrement rigoureux* ».

Ainsi, la CNIL craint que le texte de loi n'apporte aucune garantie

> « à *l'équilibre entre les droits des citoyens et les prérogatives de l'Etat [...] Il est difficile d'apprécier si les moyens proposés sont adéquats, pertinents et proportionnés aux objectifs poursuivis. On peut même s'interroger sur l'utilité de certains d'entre eux* ».

Egalement, la CNIL a émis des réserves à l'égard de plusieurs dispositifs dans ce projet de loi, à savoir :

- L'article 4 du projet de loi prévoit d'étendre les contrôles automatisés des véhicules qui donnent aux services de police et de gendarmerie la possibilité de photographier les conducteurs et les passagers. Pour la CNIL, il s'agit d'une « atteinte au principe fondamental de la liberté d'aller et venir ».
- Le développement de la vidéosurveillance ;
- La mise sous surveillance du téléphone et des connexions Internet dans les cybercafés (donc le développement de la cybersurveillance).
- Le contrôle, en dehors des frontières de l'UE, des voyageurs qualifiés « à risque ».

G. Maroc : La Commission Nationale de contrôle de la protection des Données (CNDP)

1) Contexte

La Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP) a été créée par la loi n°09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

C'est une commission marocaine, chargée de vérifier que les traitements des données personnelles sont licites, légaux et qu'ils ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux de l'homme. La Commission est formée de personnalités de compétence diverses dans les domaines juridique, judiciaire et informatique.

La CNDP a pour objectif principal de veiller au respect des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel. Elle assure une mission d'information et de sensibilisation auprès des individus des organismes et des institutions publiques et privées.

Elle est également membre de l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) qui rassemble les autorités de protection des données personnelles des pays de la Francophonie et dont elle est la coprésidente en collaboration avec l'autorité belge. Le choix de ces deux pays a pour objectif le transfert de la compétence européenne vers l'Afrique à travers le Maroc. Cette collaboration a pour mission principale est de définir un référentiel encadrant le transfert de données personnelles au sein de l'espace francophone.

En 2016, la commission marocaine accueillera la Conférence Internationale des Commissaires à la Protection des Données et à la Vie Privée (CICPDVP). Cette organisation est la principale organisation internationale dans le domaine de la protection des données personnelles et de la vie privée. Elle compte 101 membres et 17 observateurs, représentants les instances spécialisées dans ce domaine. La CICPDVP tient, depuis 1978, une conférence annuelle à laquelle assistent des représentants des gouvernements, des organisations internationales, des entreprises privées, des organismes de la société civile et du monde universitaire.

2) Les missions principales de la CNDP

La CNDP assure plusieurs missions autour de cinq axes principaux à savoir :

- **Information et sensibilisation** :
  La CNDP informer les personnes physiques sur les droits que leur confère le nouveau cadre juridique réglementant l'utilisation de leurs données personnelles au Maroc. Elle conseille et accompagne les individus en vue de se prémunir contre tout abus d'utilisation de leurs données personnelles. Egalement la CNDP sensibilise les organismes

publics et privés sur leurs obligations et les meilleures pratiques en matière de traitement des données personnelles ;

- **Conseil et proposition aux institutions publiques et privées :**
  La CNDP assure une mission de conseil auprès du gouvernement, du parlement et des autres administrations sur les aspects relatifs à la protection des données personnelles. A cet effet, elle donne son avis sur les projets et propositions de lois et de règlements relatifs au traitement des données à caractère personnel, elle aide le gouvernement à préparer la position marocaine lors des négociations internationales en la matière et présente au gouvernement toute suggestion ou proposition de législation ayant trait à la protection d'informations nominatives ;
- **Protection des données personnelles :**
  A ce titre, a CNDP œuvre à l'instauration d'une meilleure transparence dans l'utilisation des données personnelles par les organismes publiques et privées et à garantir l'équilibre entre le respect de la vie privée des individus et le besoin des organismes d'utiliser les données personnelles dans leurs activités ;
- **Contrôle et investigation des traitements:**
  La CNDP est dotée de pouvoirs d'investigation et d'enquête lui permettant de contrôler et de vérifier que les traitements des données personnelles sont effectués conformément aux dispositions de la loi 09-08 et de ses textes d'application.
- **Veille juridique et technologique :**
  La CNDP surveille, étudie et analyse les tendances et les mutations technologiques, économiques, juridiques et sociétales pouvant affecter la protection des données personnelles au Maroc.

3) Composition des membres de la CNDP:

- Un président, nommé par le Roi via un dahir [(1)] ;
- Six membres, nommés également par le Roi, suite à une proposition :
  - Du Premier ministre (deux membres) ;
  - Du président de la Chambre des représentants (deux membres) ;
  - Du président de la Chambre des conseillers (deux membres).

Les membres de la commission sont désignés pour une période de cinq ans, renouvelable une seule fois.

[(1)] Dans Larousse, un dahir est un « diplôme, brevet, privilège, l'acte qui contient la concession d'un privilège ». Dans Wikipédia, on trouve la définition suivante : « Un dahir ou dahir chérifien est un décret royal. Dans la législation marocaine ce terme désigne le sceau du roi apposé sur les textes de lois votés au parlement. D'autres décrets royaux prennent la nomination dahir, tels que les nominations aux emplois supérieurs ».

H. Comparaison des champs d'intervention de la CNDP et de la CNIL

La création de la CNPD marocaine était inspirée de l'expérience de la CNIL en France. En effet, en créant la CNDP, le Maroc devient le premier pays africain à mettre en place une instance dédiée à la protection des données personnelles et ainsi le Maroc confirme son « leadership » dans le numérique au niveau africain. Cette création a également pour objectif également de confirmer le statut avancé accordé au Maroc par l'Union européenne qui insiste sur la nécessité pour Rabat de se doter d'une telle Commission. Cette position du Maroc est soutenue pour la France, pays historiquement proche du royaume.

Si nous regardons les statuts juridique de des deux instances, CNDP et CNIL, nous remarquons une certaine convergence dans les missions et les finalités des travaux, cependant, leur périmètre d'intervention n'est pas le même.

En effet, la CNIL, comme commission de lois et libertés pourrait intervenir voir sanctionner dans le cadre de ces travaux sur l'ensemble des secteurs impliquant des activités numériques. La CNDP marocain, elle n'est pas en mesure d'annoncer de sanctionner ou d'apporter son regard sur l'ensemble des secteurs par exemple sur le fonctionnement des instances de sécurités marocaines. Elle ne peut pas porter un avis sur des activités de surveillance comme c'est le cas en France pour la CNIL. Cette différenciation est due principalement aux différences des contextes et des régimes politiques entre les deux pays ne permettent pas à la CNDP marocaine d'avoir le même poids et influence que son homologue français.

Nous notons cependant que le CNDP intervient en ce qui concerne la protection des données personnelles des citoyens par les organismes opérants sur le territoire marocain selon les dispositifs garantie par la loi du 09-08 apparu dans le Bulletin Officiel (BO) n°5714 du 05-03-2009 comme la vidéosurveillance au travail, la collecte des données à des fins publicitaires, etc. Son rôle est restreint sur le contrôle et transmission des dossiers aux tribunaux administratifs pour décision. Elle a seulement un rôle de contrôle et surtout du conseil auprès des instances administratives. Cependant, le domaine lié à la sécurité, au service de renseignement et à l'armée sont hors son champ d'intervention. D'ailleurs, nous avons remarqué une rareté d'information par rapport à ces domaines, ce qui confirme qu'il s'agit d'un champ d'action très fermé. Contrairement à la CNIL, qui est une autorité autonome agissant pour que l'informatique, dans la sphère privée ou professionnelle, soit au service du citoyen afin de préserver ses droits fondamentaux de liberté et de vie privée.

A signaler que les deux instances font partie des membres de la G29 même si le Maroc ne fait pas partie des pays européens. Son adhésion est soutenue par les homologues français.

I. Travaux du groupe G29

Le G29 ou Groupe de travail Article 29 sur la protection des données (en anglais Article 29 Data Protection Working Party) est un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ainsi, l'article 29 de la directive 95/46/CE est comme suit:

[Article 29 de la directive 95/46/CE]

« Groupe de protection des personnes à l'égard du traitement des données à caractère personnel :

- *Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé «groupe».*
- *Le groupe a un caractère consultatif et indépendant.*
- *Le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission.*
- *Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci procèdent à la nomination d'un représentant commun. Il en va de même pour les autorités créées pour les institutions et organismes communautaires.*
- *Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle.*
- *Le groupe élit son président. La durée du mandat du président est de deux ans. Le mandat est renouvelable.*
- *Le secrétariat du groupe est assuré par la Commission.*
- *Le groupe établit son règlement intérieur.*
- *Le groupe examine les questions mises à l'ordre du jour par son président, soit à l'initiative de celui-ci, soit à la demande d'un représentant des autorités de contrôle ou de la Commission. »*

Son organisation et ses missions sont définies par les articles 29 et 30 de la directive 95/46/CE, dont il tire sa dénomination, et par l'article 14 de la directive 97/66/CE dont voici les détails:

[Article 30 de la directive 95/46/CE]

« *Le groupe a pour mission:*

- *d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en œuvre homogène;*

- *de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers;*

- *de conseiller la Commission sur tout projet de modification de la présente directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés;*

- *de donner un avis sur les codes de conduite élaborés au niveau communautaire.*

- *Si le groupe constate que des divergences, susceptibles de porter atteinte à l'équivalence de la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté, s'établissent entre les législations et pratiques des États membres, il en informe la Commission.*

- *Les avis et recommandations du groupe sont transmis à la Commission et au comité visé à l'article 31.*

- *La Commission informe le groupe des suites qu'elle a données à ses avis et recommandations. Elle rédige à cet effet un rapport qui est transmis également au Parlement européen et au Conseil. Ce rapport est publié.*

- *Le groupe établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté et dans les pays tiers, qu'il communique à la Commission, au Parlement européen et au Conseil. Ce rapport est publié.* »

[Article 14 de la directive 97/66/CE]

« Extension du champ d'application de certaines dispositions de la directive 95/46/CE]

- *Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus aux articles 5 et 6 et à l'article 8 paragraphes 1 à 4 lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de l'utilisation non autorisée du système de télécommunications, comme le prévoit l'article 13 paragraphe 1 de la directive 95/46/CE.*

- *Les dispositions du chapitre III de la directive 95/46/CE, relatif aux recours juridictionnels, à la responsabilité et aux sanctions, sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.*

- *Le groupe «protection des personnes à l'égard du traitement des données à caractère personnel» institué par l'article 29 de la directive 95/46/CE remplit les tâches visées à l'article 30 de ladite directive également en ce qui concerne la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des télécommunications, qui est l'objet de la présente directive.»*

Le groupe G29, dont fait partie la France, à travers la CNIL, et le Maroc , par la CNDP, réalise des consultations publiques entre les différents membres de l'institution afin d'aider à préconiser les bonnes pratiques en matière de traitement des données personnelles des citoyens des pays membres. Le travail de ce groupe consiste également à mettre en place une législation commune et des partenariats entre les pays membres afin d'harmoniser les pratiques juridiques concernant les données personnelles.

J. Travaux de la Chaire Valeurs et politiques des informations personnelles

La Chaire Valeurs et politiques des informations personnelles a été inaugurée le 9 avril 2013 à l'institut Mines-Télécom. Cette chaire pluridisciplinaire est co-animée par des enseignants-chercheurs de Télécom École de Management, Télécom ParisTech et Télécom SudParis.

La Chaire se propose d'aider, entre-autres, les pouvoirs publics dans leurs réflexions sur la collecte, l'utilisation des informations personnelles, à savoir les informations concernant les individus : leurs vies privées, leurs activités professionnelles, leurs identités numériques, leurs contributions sur les réseaux sociaux, *etc*.

Ainsi les travaux de la chaire sont pluridisciplinaires, ils concernent les domaines suivants:

- ***Domaine de la philosophie et de l'éthique*** **:**
  La chaire apporte un regarde philosophique et éthique sur la question du traitement des données personnelles. En effet, Pierre-Antoine Chardel, membre de la chaire, considère que *« L'expansion du numérique dans nos vies appelle des formes de responsabilité qui concernent la signification que nous souhaitons préserver dans le développement de nos sociétés. La question de la protection des informations personnelles est, à cet égard, cruciale dans la mesure où elle concerne la façon dont nous entendons nous inscrire (de manière consumériste ou responsable) dans nos environnements technologiques complexes* ».

- ***Domaine du Droit*** **:**
  En effet, la chaire souhaite apporter des réponses à des questions de l'ordre juridiques. L'enjeu pour la chaire consiste à assurer le respect des droits et des libertés fondamentales des citoyens en adéquation avec le système juridique : respect de la vie privée et de l'identité humaine, protection des données à caractère personnel, liberté de déplacement, liberté d'expression, etc.

- ***Domaine de l'économie*** **:**
  A travers ses travaux, la chaire souhaite apporter un regard économique par rapport à l'économie des données personnelles. En effet, selon Patrick Waelbroeck, membre de la chaire, « *L'analyse coût/bénéfice des données « autonomes » ouvrira ensuite la voie à des questionnements sociétaux et philosophiques autour de la notion de marché des données personnelles. Enfin les recherches en économie analyseront les enjeux économiques, les business models et les écosystèmes des données connectées à travers le big data, le cloud et l'internet des objets* ».

- ***Domaine des sciences et de l'informatique*** **:**
  La chaire souhaite apporte un regarde scientifique et technique par rapport aux mécanismes de production, de traitement et de protection des données personnelles. L'objectif est de concevoir des outils technologiques visant à aider les acteurs à prendre

des décisions éclairées concernant la gestion des données personnelles conformément au cadre réglementaire en vigueur.

Dans le cadre de nos recherches, nous avons eu l'occasion de participer aux travaux de la chaire dont notre directeur de thèse fait partie des membres-fondateurs.
Nous avons pu exposer nos travaux au sein de cette chaire en Juin 2013 (voir annexe pour plus de détails).

Nous avons également suivi l'ensemble des publications et conférences de la chaire ce qui nous a permis de comprendre les enjeux liés aux données d'un point de vue juridique, économique, philosophique, social et technique.

Nous mettons à disposition une description des travaux réalisés et les différentes interventions dans la cadre de cette chaire de recherche.

K. Initiatives de l'Association Quadrature du Net

a) Création de l'association

La Quadrature du Net (abrégé LQDN) est une association de défense des droits et libertés des citoyens sur Internet. Elle est fondée en 2008 et intervient dans les débats concernant la liberté d'expression, le droit d'auteur, la régulation du secteur des télécommunications, ou encore le respect de la vie privée sur Internet. Cette association s'est fait connaître par son opposition aux lois HADOPI en 2008 et aux différentes lois liées au renseignement dont la dernière voté en 2015.

À l'échelle européenne et mondiale, son action a porté en particulier sur le Paquet Télécom[(1)], le traité ACTA[(2)], et se fait principalement entendu par ses positions par rapport au débat autour de la neutralité du Net.

Ainsi, selon les statuts fondateurs de l'association Quadrature de Net, nous avons les articles principaux suivants :

> **[Article 1 : Constitution]**
> « *Il est fondé entre les adhérents aux présents statuts une Association régie par la loi du 1er juillet 1901 modifiée et ses textes d'application. La durée de l'Association est illimitée* ».
>
> **[Article 3 : Objet]**
> *L'Association a pour objet désintéressé et non lucratif […] de mener une réflexion, des études, analyses, actions pour la défense des libertés individuelles sur internet […] d'aider les citoyens à comprendre le fonctionnement de l'internet […] ».*
>
> **[Article 14]**
> « *L'Association peut être dotée d'un Conseil Scientifique. […] Le Conseil Scientifique a pour but de développer une veille scientifique et une réflexion active sur les usages d'internet, les projets de loi, les lois et règlements votés et toute matière pouvant intéresser l'Association […]* »

---

(1) Le paquet télécom est un ensemble de directives européennes régulant le secteur des télécommunications qui proposent notamment de renforcer les droits des consommateurs, d'élargir les compétences des régulateurs nationaux, ou encore des mesures visant à accélérer le développement du très haut débit et à réduire le « fossé numérique » entre zones rurales et zones urbaines.

(2) ACTA (pour Anti-Counterfeiting Trade Agreement), est un traité international multilatéral sur le renforcement des droits de propriété intellectuelle, négocié de 2006 à 2010 par une quarantaine de pays dont la France et le Maroc.

b) L'association et la cybersurveillance

i. Position par rapport au projet de loi relatif au renseignement

L'association « Quadrature de Net » estime que l'adoption de la loi relative au renseignement « légalise la surveillance de masse et avalise un recul historique des droits fondamentaux ». En effet, l'association s'est opposée principalement à l'utilisation des boîtes noires ainsi qu'aux algorithmiques associés. Ainsi, elle juge qu'en adoptant cette loi, l'État légalise une surveillance de masse au niveau national et internationale. Une situation, qu'elle juge, non conforme à la Constitution.

Ainsi, l'association considère que plusieurs dispositions sont ainsi directement inspirées du droit et des pratiques de la NSA en installant des mécanismes de surveillance de masse notamment avec les dispositifs techniques d'analyse automatique du trafic Internet en vue de détecter des « comportements suspects » (art. L. 851-3) ou le régime de surveillance dite « internationale » (art. L. 854-1) qui permet la collecte des données et des correspondances.

L'association estime également que c'est une volonté politique de systématiser le piratage informatique hors des frontières en s'inspirant encore une fois des pratiques des agences anglo-saxonnes. Enfin, elle estime également que le texte est à plusieurs égards en recul par rapport au droit et à pratiques existantes, dans la mesure notamment où certaines modalités fondamentales du contrôle actuellement exercé par la commission du contrôle sont démantelées, tandis que le champ d'intervention des services est largement étendu.

ii. Position par rapport au projet de loi anti-terroriste

L'association Quadrature du Net s'est opposé publiquement au projet de loi de lutte contre le terrorisme. Ainsi, elle estime que « la plupart des articles contenus dans ce projet de loi instaurent des mesures disproportionnées ou inefficaces au regard de l'équilibre indispensable à conserver, dans une démocratie, entre libertés publiques et lutte contre le terrorisme ». En effet, la Quadrature du Net s'oppose au texte dans son ensemble qu'elle considère indigne qu'un texte aussi lourd de conséquences soit examiné en procédure d'urgence, avec une seule lecture par le Parlement et sans débat national.

L'association estime que « les nombreux articles du projet de loi s'attaquant à nos libertés fondamentales et l'extra judiciarisation de la répression sur Internet doivent être supprimés ou revus dans le respect de l'État de droit et des principes démocratiques ».

C'est ainsi que l'association Quadrature du Net porte un regard critique vis-à-vis la réglementation du monde numérique et un regard particulièrement pertinent par rapport aux lois concernant le renseignement et le terrorisme. Sa mobilisation continue ainsi que leur travail pour vulgariser les dangers et les risques d'une adoption rapide sans débats nationaux est remarquable.

2. Chapitre 2 : cybersécurité et cybersurveillance à l'ère du Cyber-État

Dans le contexte de lutte contre le terrorisme sous toutes ses formes, le débat politique , en France comme au Maroc, est agité par une inquiétude grandissante autour du déploiement de dispositifs numériques de surveillance généralisée, par l'adoption de plusieurs dispositifs légaux (loi anti-terrorisme, loi relative au renseignement, …) ainsi que par les révélations d'Edward Snowden ou de Wikileaks sur les affaires de surveillance en masse comme le programme PRISM ou les affaires SWIFT.

Ainsi, le grand public a découvert l'étendue des interceptions auxquelles les services de renseignement des régimes « démocratiques » occidentaux ont soumis leurs propres citoyens mais également nous avons pu découvrir des programmes de surveillance entre États-amis à l'image de la mise sur écoute par la NSA (National Security Agency) de la chancelière allemande Angela Merkel et de la présidente brésilienne Dilma Rousseff.

A travers cette section, nous allons aborder la notion de cyberspace en tant que « lieu » immatériel où se déploient les enjeux politiques du numérique, des intérêts économiques et stratégiques qui promeuvent des méthodes de surveillance, sous prétexte de lutte contre le terrorisme, voire le cyberterrorisme, et la cybercriminalité et non comme continuité des outils de contrôle des populations adoptés depuis longtemps par les États dits « modernes ».

Ainsi, nous allons aborder les notions de cyberspace et de toutes les notions liées à la cybersécurité comme cyberdéfense, cyberguerre et cybermenace.

Après avoir abordé a notion de cybersurveillance et comment elle se déploie massivement, nous détaillerons les révélations de Snowden pour comprendre l'utilisation des technologies numérique par la NSA (National Security Agency).

Dans ce contexte de surveillance et des Cyber-États, nous essayons de comprendre la notion de la souveraineté et comment un nouveau concept pourrait en émerger dans le contexte actuel à savoir : cybersouveraineté.

Par la suite, nous essayerons de voir comment l'État pourrait se confirmer dans ce contexte de lutte contre le terrorisme et de surveillance de masse et son articulation avec la notion de *sécurité nationale*.

A. Cybersécurité à l'ère du Cyber-État

a) Le cyberspace à l'ère du Cyber-État

Le cyberspace est un objet d'étude lié à une multitude de définitions dans les mondes universitaire et militaire[1]. En effet, le cyberespace est considéré comme un environnement[2], un domaine[3], un théâtre d'opérations, un espace[4], un substrat[5] , ou encore un milieu ou un moyen[6]. Ainsi, ce terme est considéré stratégique pour plusieurs auteurs et souvent utilisé dans les négociations internationales.

Ainsi, pour Pierre Levy[7], le cyberspace est considéré comme étant l'univers des réseaux numériques, un lieu de rencontre et d'aventures, un enjeu pour des conflits mondiaux et des nouvelles frontières économiques et culturelles. Comme le souligne Alix Desforges[8], le cyberspace est un espace plus englobant et plus virtuel. Il est à la fois un monde virtuel, dématérialisé, sans frontières, anonyme, de libertés, de partage et de communication.

En effet, on peut y voir un espace de progression, de démocratie et de progrès économique ; mais il peut être aussi à la fois un espace où l'on pratique une surveillance de masse, un contrôle des foules. Cette représentation confirmée et réveillée essentiellement par les pratiques de la NSA révélées par Edouard Snowden comme nous allons le voir dans la suite et le développement du cyberterrorisme.

Ainsi, le cyberspace est lié principalement à deux références principales : « Internet » et « Espace ». En effet, comme nous l'avons vu précédemment, l'interconnexion des réseaux mondiaux forment l'Internet d'aujourd'hui qui constitue une partie de cyberspace. Par la suite, la référence spatiale de la cyberspace peut être un espace, un monde, un milieu ou un environnement. Ainsi, le cyberspace a une dimension géographique sans, pour autant, être un lieu ou un territoire géographique déterminé[9].

---

(1) D. BETZ et T. STEVENS, Cyberspace and the State, Toward a Strategy for Cyberpower, The International Institute for Strategic Studies, Routledge, Londres, 2011.

(2) R. HARKNETT, Leaving Deterrence Behind: Warfighting and National Cybersecurity, in, Journal of Homeland Security and Emergency Management, March 2010.

(3) J. CARR, Inside Cyber Warfare: Mapping the Cyber Underworld, O'Reilly Media, 2011.

(4) O. KEMPF, Introduction à la cyberstratégie, Economica, 2015.

(5) C. DEMCHAK, Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI), Center for Cyber Conflict Studies, US Naval War College, 2012.

(6) M. LIBICKI, Crisis and Escalation in Cyberspace, Santa Monica, Rand, 2012.

(7) P. LEVY, L'Intelligence collective : Pour une anthropologie du cyberspace, La Découverte, 1994.

(8) A. DESFORGES, Les représentations du cyberespace: un outil géopolitique, La Découverte, Paris, 2014.

(9) A. DESFORGES, Les représentations du cyberespace: un outil géopolitique, La Découverte, Paris, 2014.

De ce fait, pour plusieurs chercheurs, il s'agirait ainsi d'une entité à part, souvent qualifiée de virtuelle, qu'il conviendrait de relier au réel pour analyser les conflits qui en découlent. Une position confirmée principalement par les travaux de recherches menées en relations internationales par Joseph Nye[(1)].

Ainsi, le mot cyberspace est inventé par William Gibson, lui-même inspiré par les travaux de Wiener. Comme nous l'avons vu, en 1948, Norbert Wiener développait l'idée que l'information et la communication sont résolument nécessaires au fonctionnement de la société. Il écrivait : « *La communication est le fondement de la société et ceux dont le travail consiste à maintenir libres les voies de communication sont ceux-là mêmes dont dépend surtout la pérennité ou bien la chute de la civilisation* »[(2)].

Ainsi, la représentation d'un cyberespace comme étant un espace de liberté, et de promotion de la démocratie est omniprésent dans les discours des instances de gouvernance internationale comme nous le verrons dans la *section 3*. Ainsi, pour le préserver comme espace de démocratie et de liberté, 54 pays[(3)] ; parmi lesquels les États-Unis, le Royaume-Uni, la France et le Maroc ont refusé de signer le texte révisant le règlement des télécommunications internationales. Ainsi, Fleur Pellerin, ministre de l'Économie numérique (2012-2014), déclarait alors : *« Internet est un bien commun, qui doit rester libre et ouvert. Nous ne pouvions pas signer un texte qui soulevait de telles inquiétudes auprès des organisations non gouvernementales et des acteurs du numérique* »[(4)]. Ce texte de révision est largement soutenu par la Chine et la Russie. Ainsi, promouvoir le cyberespace comme espace de liberté a été un outil puissant de la stratégie américaine pour mettre un frein aux velléités russes et chinoises de contrôle sur le réseau mais aussi pour conserver leur position dominante dans la gouvernance de l'Internet alors que celle-ci est de plus en plus critiquée.

Cependant, le sentiment d'insécurité est permanent dans un environnement cyberspace. En effet, des actions criminelles peuvent être commises à l'encontre des États et des entreprises mais également à l'encontre des simples citoyens. On parle alors de la cybercriminalité ou de la *cybermenace* (nous y reviendrons dans la prochaine partie). Ainsi, une attaque d'un hacker informaticien peut mettre à genoux les systèmes d'un État sans que cela puisse arriver aussi facilement dans la vraie vie. Cependant, comme Olivier Kempf le précise « cette perception est renforcée par toute la littérature, écrite ou filmée, qui est pleine de ce genre de scénarios »[(5)].

---

(1) J. NYE, The Futur of the Power , Public Affairs, U.S.A , 2011.

(2) N. WIENER, « Cybernétics or control and communication in the animal and machine», 1948.

(3) Parmi les pays signataires, nous retrouvons la Russie, la Chine, l'Iran, L'Arabie Saoudite, …, une majorité des régimes qualifiés de « non démocratiques».

(4) F. BERGE, «Le sommet de Dubaï entérine la fragmentation de l'Internet mondial», Revue 01Net, 17 décembre 2012.

(5) O. KEMPF, Introduction à la cyberstratégie, Economica, 2015, P.138.

Il nous semble donc nécessaire de relativiser l'éventualité pour qu'une situation pareille puisse arriver pour plusieurs raisons : l'interconnexion des systèmes est de plus en plus complexe, la nécessité d'avoir des compétences très pointues, les États et les grandes entreprises participent à limiter ces attaques en investissant dans leur systèmes de sécurité.

Ainsi, la difficulté d'identifier les menaces dans un cyberspace fait naitre des débats vifs autour de la cyberguerre dans un espace où les frontières entre les États sont floues ou inexistante. Ainsi, Bertrand Boyer souligne que « *entretenant les peurs et les craintes liées aux nouvelles technologies, jouant sur la confusion entre la guerre (entre États), la criminalité (fût-elle organisée) et la compétition économique, elles [les publications alarmistes] contribuent à l'enracinement de la croyance en une arme absolue capable d'offrir une réponse à tout type d'attaque* »[(1)]. Alors que dans ce contexte, nous avons remarqué l'augmentation constante des moyens humains et financiers dévolus à ces questions de la cyberguerre et de la cybersécurité. Ainsi, comme nous l'avons vu, Jean-Yves Le Drian, ministre de la Défense, annonçait au Forum international sur la cybersécurité, en janvier 2014, la mise en place d'un « *plan Défense cyber* » d'un budget d'un milliard d'euros en arguant que « *devant des menaces majeures, qui peuvent aller jusqu'à de véritables actes de guerre, militaires ou non directement militaires, il y a un enjeu de premier ordre pour la défense, la souveraineté et la sécurité de notre nation* »[(2)].

Pour finir, nous remarquons que la cyberspace véhicule plusieurs représentations et se voient renforcer avec l'arrivée des nouveaux outils comme le Cloud Computing et le Big data. Cependant, les différentes conceptions de cyberspace sont retranscrites dans les stratégies - militaires soient-elles - des États, qui, de plus en plus, s'approprient des compétences nécessaires pour développer leurs propres outils de cyberguerre et de cyberdéfense.

---

(1) B. BOYER, Cyberstratégie : l'art de la guerre numérique, Nuvis, Paris, 2012.

(2) H. MEDDAH, «Au FIC, Le Drian soigne sa cyberdéfense », L'Usine digitale, 22 janvier 2014.

b) De la construction d'une cybermenace

Depuis les années 90, John Arquilla et David Ronfeldt[(1)], prévoyait le déclenchement d'une cyberguerre suite au développement des technologies de l'information et de communication. En effet, depuis des années 2000, nous assistons à une diffusion massive des discours étatiques concernant la cyberguerre au sein du cyberspace. Ce dernier, cyberspace, est identifié par le Livre blanc sur la défense et la sécurité nationale de 2013 comme un « *champ de confrontation* » et devient le terrain de conflits de cyberguerre et de cyberdéfense, ainsi, faisant naitre de nouveaux concepts, à savoir la cybermenace et le cyberterrorisme.

Comme le note Myriam Dunn Cavelty[(2)], l'utilisation massive du préfixe cyber- consiste avant tout à désigner une action qui se fait par l'utilisation d'ordinateurs. En effet, ces ordinateurs peuvent être déployé dans une architecture Cloud tout en intégrant des technologies Big data.

Ainsi, Le Livre blanc français de 2013 identifie trois types de cybermenaces :

- *La cybercriminalité qui ne relève pas spécifiquement de la sécurité nationale:* Ce type d'attaque vise principalement les particuliers et les entreprises privées. Il consiste à pirater des informations personnelles, de dérober des données bancaires, etc. ;
- *Les tentatives de pénétration de réseaux numériques à des fins d'espionnage* : Ce type d'attaque vise les entreprises et les administrations publiques et principalement conduit par des organisations étrangères. L'objectif recherché est d'espionner les communications et avoir accès à des informations confidentielles ;
- *Les attaques visant le sabotage de systèmes d'importance vitale* : Ce type d'attaque vise à déstabiliser le fonctionnement d'un État. Ils peuvent être considérés comme un acte de guerre. Ainsi, il s'agit d'une atteinte à la souveraineté du pays.

A cela s'ajoute d'autres éléments identifiés par le directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), en effet, il s'agit de :

- *La déstabilisation conduite par des attaques de type « defacement* » : cela consiste à modifier les pages d'un site pour faire apparaître une revendication ;
- *Déstabilisation par déni de service* qui consistent à rendre inaccessible un site Web en le saturant de requêtes ;
- *Publication d'informations dérobées* qui consiste à divulguer en ligne sur Internet les informations confidentielles piratées.

---

(1) J. ARQUILLA et D. RONFELDT, « Cyberwar is coming ! », Comparative Strategy, 1993.

(2) M. DUNN CAVELTY, *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Routledge, Abingdon, 2008.

Cependant, nous remarquons que les mêmes techniques d'attaque pouvant être utilisées dans le cadre d'une cyberguerre (attaque d'espionnage par exemple) ou de simple acte de cybercriminalité (pirate des données bancaires par exemple). Malgré cette difficulté d'identification de sa typologie, très peu d'attaques ont eu des conséquences significatives sur la sécurité nationale de la France ou du Maroc, du moins parmi celles qui ont été portées à la connaissance du public.

Ainsi, nous considérons que la France est plus vulnérable à ce type d'attaque que le Maroc de part de la croissance des interconnexions de ses réseaux informatiques considérés comme le « système nerveux » de l'État français.

Cependant, comme le précise Myriam Dunn Cavelty[(1)], de nombreux États ont placé les questions de cybersécurité et de cyberdéfense au premier plan de leur agenda politique en les liants aux questions de sécurité nationale. En effet, En France, le fait que le Livre blanc sur la défense et la sécurité nationale de 2008 place la sécurité des systèmes d'information au même niveau stratégique que la dissuasion nucléaire illustre l'importance prise par ces questions pour des décideurs stratégiques et politiques. Le Maroc de son côté et pour faire face à cette menace, il s'est doté d'un comité stratégique de la Sécurité des systèmes de l'information et d'une Direction générale de la Sécurité de systèmes de l'information (DGSSI). Ainsi cette autorité nationale de sécurité des systèmes d'information, comportant un centre de veille, de détection et de réaction aux attaques informatiques a élaboré une stratégie nationale de Cybersécurité qui comporte une série de mesures visant à élever et homogénéiser les niveaux de protection et de maturité de la sécurité de l'ensemble des systèmes d'information des administrations marocaines.

[(1)] M. DUNN CAVELTY, *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Routledge, Abingdon, 2008.

c) Cybersurveillance à l'ère du Cyber-État

Désignée par l'Organisation des Nations Unies comme la nation la plus avancée en Europe et quatrième dans le monde, pour l'administration numérique, la France s'inscrit comme un acteur majeur dans le développement du domaine numérique au niveau mondial. Ainsi, plus de la moitié des citoyens français (53%) paient leurs impôts sur Internet, et 93 % effectuent leur demande d'extrait de casier judiciaire en ligne et plus de 80 % des agriculteurs effectuent des demandes d'aide au titre de la Politique Agricole Commune (PAC) via Internet. Des données qui confirment la position de plus en plus dominante qu'occupe le Cyber-État.

Ainsi, les données personnelles concernant les activités des citoyens dans le Cyber-État: la santé, l'emploi, les revenus, les communications, les voyages et les déplacements sont officiellement enregistrées. Et, les récentes révélations ont montré que même si l'État central, français ou marocain, ne s'en charge pas, d'autres États espionnent.

De ce fait, le terme cybersurveillance désigne la surveillance du Net ou une surveillance permise par une architecture de type cybernétique au sens de Nobert Weiner. Ainsi, elle s'exerce par le biais d'Internet en rendant transparentes les activités des personnes surveillées. Elle vise cependant moins à contraindre ou à interdire qu'à anticiper les comportements des individus à partir de leurs activités en ligne, en vue de prévenir des crimes ou des actes de délinquance. L'indexation des traces numériques laissées au gré des navigations sur Internet devenant ainsi le socle de ce nouveau type de surveillance[(1)].

Ainsi, la surveillance, dans sa pratique, a servi dans le passé à l'implantation des régimes totalitaires[(2)] à l'image du régime Nazi, de L'Union Soviétique stalinienne, la Chine de Mao Tsé- Toung, et le pouvoir de Franco en Espagne, *etc*. Alors qu'aujourd'hui, avec le développement des techniques sophistiquées de surveillance et plus précisément avec le Cloud et le Big data, nous ne remarquons pas des dérives totalitaires, en tout cas, dans les sociétés dites démocratiques.

---

(1) G. PERIES, La confiance au prisme de la « sécurité nationale». Une analyse critique à l'ère des réseaux numériques, Politiques sécuritaire et surveillance numérique, P-A CHARDEL (Coord), Paris, Hermès, 2014, P.59.

(2) Nous entendrons ici par « *totalitarisme* » un régime politique centralisé qui détruit totalement la diversité du tissu social au nom d'un idéal d'organisation collective et homogène.

Ainsi, comme il faut le rappeler, la surveillance s'est instituée progressivement en même temps que l'État de droit dès la fin du XVIIIe siècle et au début du XIXe siècle[(1)]. Comme Michel Foucault[(2)] l'indique, l'apparition du mot « surveillance » et la généralisation de l'usage du verbe «surveiller» correspondent à la mise en place d'un État de droit en précisant qu'il faut à la fois enseigner les lois et s'assurer qu'on les respecte. Ainsi, nous pouvons considérer que la cybersurveillance s'institue progressivement en même temps qu'avec le Cyber-État.

Aujourd'hui, les technologies de Cloud Computing et de Big data permettent une collecte massive des données ainsi la mise en place d'une cybersurveillance permet la production massive d'informations sur l'individu afin d'établir des profils de plus en plus atomisés et précieux pour les entreprises marchandes. Or la cybersurveillance et les techniques de profilage rendues performantes grâce au Cloud et «Big Data» ne sont pas seulement utilisées dans le contexte commercial, mais aussi dans les stratégies de sécurité. Ainsi, selon Marx Weber, l'État, « entreprise qui revendique avec succès » son monopole de la violence légitime, lorsque le citoyen obéit à son autorité (rapport obéissance-autorité). En effet, selon McGinnis[(3)] les mécanismes du Big data garantiraient le maintien de l'autorité de L'État et ce de manière plus flexible que les mécanismes rigides du modèle bureaucratique propre à la modernité politique. Nous pouvons considérer que cette obéissance à l'autorité de l'État grâce au Big data constitue le socle techno-logique du Cyber-État.

---

(1) J-G GANASCIA, De la surveillance à la surveillance, Politiques sécuritaire et surveillance numérique, et P-A CHARDEL (Coord), Paris, Hermès, 2014, P.119.

(2) M. FOUCAULT, Surveiller et punir, Naissance de la prison, Paris, Gallimard, 1975.

(3) J. MCGINNIS, Accelerating Democracy: Tranforming Governance Through Technology, Princeton University Press, 2012.

d) Retour sur l'affaire Snowden

L'affaire Snowden a permis de rendre publiquement par l'intermédiaire des médias, notamment Le Guardian[(1)] et le Washington Post[(2)], des informations classées top-secrètes de la *NSA*[(3)] concernant des programmes de surveillance de masse comme *SIWFT*[(4)], *PRISM*[(5)].

En effet, ces révélations ont montré que les collectes massives d'informations par la NSA, concernant des citoyens du monde entier, dépassent le cadre de la lutte nécessaire contre le terrorisme ou contre la cybercriminalité mais ils s'inscrivent dans une continuité des programmes de surveillance par les États-Unis depuis la deuxième guerre mondiale. Ainsi, Snowden justifie ses actions en indiquant que son « *seul objectif est de dire au public ce qui est fait en son nom et ce qui est fait contre lui* »[(6)].

---

(1) Glenn Greenwald, Ewen MacAskill et Laura Poitras, « Edward Snowden: the whistleblower behind the NSA surveillance revelations », The Guardian, 10 juin 2013.

(2) Barton Gellman, Aaron Blake et Greg Miller, « Edward Snowden comes forward as source of NSA leaks»,The Washington Post, 9 juin 2013.

(3) La National Security Agency (NSA, « Agence nationale de la sécurité ») est un organisme gouvernemental du département de la Défense des États-Unis, responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information et de traitement des données du gouvernement américain.

(4) Acronyme de la Society for Worldwide Interbank Financial Telecommunication qui renvoie à l'autorisation donnée en 2007 aux USA par l'UE de contrôler l'ensemble des transactions bancaires qui transite par cette plateforme en entérinant des pratiques existantes depuis 2002 dans le cadre de la lutte contre le terrorisme.

(5) PRISM, également appelé US-984XN1, est un programme de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques. Ce programme relevant de la National Security Agency (NSA) prévoit le ciblage de personnes vivant hors des États-Unis10. PRISM est supervisé par la United States Foreign Intelligence Surveillance Court (FISC) conformément au FISA Amendments Act of 2008 (FISA).

(6) Tanguy Berthemet, « Edward Snowden, l'homme qui fait trembler le gouvernement américain », Le Figaro.fr - 10 juin 2013.

Pour reprendre chronologiquement les événements :

- *Le 5 Juin 2013* : Le Washington Post et le Guardian ont publié une note secrète sous le code s.125 de *Patriot Act*[(1)] incitant l'opérateur Télécom Verizon à fournir à la NSA les détails des appels téléphoniques de tous les citoyens américains ;

- *Le 6 Juin 2013* : Les deux journaux ont révélé l'existence d'un vaste programme de surveillance de la NSA nommé PRISM permettant l'accès aux données hébergées par les grandes entreprises du web américains. Ces mêmes entreprises

- sont également les principaux fournisseurs des solutions Cloud Computing. Dans la même journée, le directeur de la NSA, ADAM Clapper, a reconnu officiellement l'existence de ce programme en précisant qu'il est lié au FISA Amendment 2008 s.1881a/702 ;

- *Le 7 Juin* : L'identité d'Edward Snowden est révélée publiquement par le Washington Post et le Guardian ;

- *Le 09 Juin 2013* : Edward Snowden, ex consultant de la NSA, a volontairement révélé les différents détails de ce programme d'espionnage dans une interview à un journal chinois.

Ainsi, cette affaire a bouleversé les rapports de confiance et précisément entre les « Cyber-États » au niveau de cyberspace en remettant en cause toute la gouvernance actuelle d'Internet. En effet, l'affaire Snowden n'est pas une simple affaire de renseignement ou une affaire seulement politique, elle a eu des conséquences géopolitiques conséquentes au niveau mondial mais également en France. Elle nous rappelle un vieux clivage géopolitique pendant la guerre d'Irak. En effet, d'un côté, les États-Unis et la Grande-Bretagne et de l'autre, la France et l'Allemagne avec un reste de monde resté neutre. Cependant, cette fois-ci, les BRICS[(2)] ont monté au créneau et ont manifesté un mécontentement à l'égard de ces pratiques des États-Unis.

---

(1) USA PATRIOT Act : Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (unir et renforcer l'Amérique en fournissant des outils appropriés pour déceler et contrer le terrorisme).

(2) BRICS est un acronyme anglais pour désigner un groupe de cinq pays qui se réunissent en sommets annuels : Brésil, Russie, Inde, Chine et Afrique du Sud. Ce sont des pays à forte croissance et le poids de leurs économies dans l'économie mondiale est significatif.

Cette affaire Snowden a eu des conséquences géopolitiques mais sans actions concrètes à l'encontre des États-Unis même si chaque pays a pris ses propres dispositifs pour assurer son autonomie et sa propre « cybersouveraineté ». En effet, dans ce contexte dominé par des solutions technologique en majorité nord-américaines, il est difficile d'être indépendant des États-Unis dans la gestion de son propre « Cyber-État ». En effet, la théorie de Joseph Nye décrivant une puissance douce « soft power »[(1)] qui viendrait à l'appui de la puissance à travers ses programmes de surveillance, a démontré qu'elle a une puissance traditionnelle mais dans un nouveau espace : Internet.

Pour faire face à ce « soft power » américain, et à l'occasion de la présentation du nouveau « *Pacte défense cyber* » par le ministre de la défense français, nous avons constaté que la première action s'intitule «*Accentuer le développement et l'usage des moyens techniques contribuant à l'autonomie de nos actions souverains* »[(2)]. En parcourant ce rapport, nous avons remarqué que le mot souverain apparait sept fois dans ce pacte ce que montre l'importance de la cyberdéfense pour la souveraineté et la « cybersouveraineté » de la France. Ça sera donc le sujet de la prochaine partie.

---

(1) Le concept de soft power désigne les méthodes d'influence développées par un Etat qui ne s'appuient pas sur la violence mais sur des éléments idéologiques ou culturels en vue de satisfaire les intérêts de la nation qui les met en œuvre. Le soft power s'exerce sous des formes de coercition, d'incitation, de séduction ou encore d'influence sur le choix des problèmes politiques apparaissant comme prioritaires, avec comme impératifs la crédibilité et la légitimité. Le terme de soft power fut pensé et décrit par Joseph S. Nye dans son ouvrage paru en 1990, Bound to Lead.

(2) Le Pacte Défense cyber a été présenté à Cesson-Sévigné (Ille-et-Vilaine) le 7 février par le ministre de la Défense. Il implique à la fois des mesures visant à accroître la mobilisation de l'ensemble du ministère de la Défense en matière de cybersécurité, ainsi que des actions destinées à soutenir les initiatives innovantes - émanant aussi bien du secteur public que privé : collectivités locales, grands groupes, PME/PMI, opérateurs de formation - et élaborées sur le modèle du Pacte Défense PME. Six axes et cinquante mesures constituent ce pacte :

- ***Axe 1*** : durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance.
- ***Axe 2*** : préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle.
- ***Axe 3*** : renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés.
- ***Axe 4*** : développer le Pôle d'excellence en cyberdéfense en Bretagne au profit du ministère de la défense et de la communauté nationale de cyberdéfense.
- ***Axe 5*** : cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance Atlantique et dans les zones d'intérêt stratégique. 15
- ***Axe 6*** : favoriser l'émergence d'une communauté nationale défense de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve

B. Souveraineté politique et cybersouveraineté à l'ère du Cyber-État

a) Contexte

La souveraineté a longtemps constitué le principe fondateur de la puissance des États. En effet, les travaux Jean Boudin au plan théorique et les traités de Westphalie au plan politique ont conçu un modèle des relations internationales et un mode de légitimation de l'exercice de pouvoir à l'intérieur des États[(1)]. Ainsi, Olivier Beaud[(2)] montre que la souveraineté de l'État moderne est liée à l'État dont elle exprime la puissance. Selon cet auteur, la souveraineté est une puissance suprême et indépendante dont le point d'appui réside dans l'acte de la souveraineté[(3)].

Avec la diffusion des technologies numériques, de nouveaux enjeux de souveraineté et d'exercice du pouvoir voient le jour avec l'apparition des nouvelles notions comme « Cyber-État » et « cybersurveillance ». Des enjeux concernant la création et l'application du droit sur le territoire national.

En effet, la territorialité de l'autorité souveraine est remise en question par le caractère dématérialisé et transfrontalier des nouveaux usages, services et échanges dans le cyberspace. Ce caractère dématérialisé prend encore forme avec la domination de grands acteurs technologiques internationaux : Américains, Chinois ou Russes. Cette domination risque d'affaiblir la capacité de l'action de l'État dans des secteurs jugés stratégique ainsi empêcher le développement des alternatives nationales (françaises ou marocaines).

D'un autre côté, l'État doit s'assurer que les libertés publiques et les droits individuels des individus sont préservés à l'ère de « Cyber-État » et de « cybersurveillance ». Ces droits fondamentaux pour une société démocratique sont de plusieurs ordres : liberté d'expression, dignité de la personne, droit à la sûreté de la personne, respect de la vie privée, droit de la propriété, *etc*. Il est donc évident que le cadre juridique assuré par les institutions de l'État n'est plus adapté à l'environnement numérique moderne qui est en constante évolution d'où la nécessité de sa revue et son adaptation aux nouvelles exigences.

---

(1) A. PECHEUL, La souveraineté dans tous ses états, Edition Cujas, Paris, 2011.

(2) O. BEAUD, La puissance de l'Etat, Paris, PUF, 1994.

(3) O. BEAUD, La puissance de l'Etat, Paris, PUF, 1994.

b) La souveraineté dans son sens général et politique

La souveraineté, dans son sens général, désigne un attribut qui est appartient à ce qui est le plus haut. Ce constat est valable pour tous les objets et compris l'autorité. En effet, cette dernière est dite souveraine, quand elle est considéré la plus haute de son domaine[(1)].

La souveraineté, dans son sens politique, appartient à l'autorité politique la plus haute, la plus élevée et placée au-dessus des autres autorités politiques. Si on considère que le pouvoir est de nature autorité politique, cela revient à dire que la souveraineté correspond au pouvoir suprême. De plus, la souveraineté politique est le droit de l'État de réglementer les activités de ses ressortissants et de les soumettre à sa contrainte et d'exercer tous les pouvoirs étatiques sur son territoire[(2)].

Par ailleurs, le concept de la souveraineté politique a été introduit pour la première fois en 1576 par Jean Bodin comme un attribut essentiel de l'État. Dans son œuvre «*Six livres de la République*», il élabore le concept clé de l'État dont l'existence se définit par la souveraineté. Pour Boudin, la souveraineté sert de pilier à l'analyse de l'État: «*La souveraineté est la puissance absolue et perpétuelle d'une République (…) c'est-à-dire la plus grande puissance de commander »*[(3)]. Dans son ouvrage « L'État fédéral et confédération d'États», le juriste français Louis Le Four donne une autre définition : « *La souveraineté est la qualité de l'État de n'être obligé ou déterminé que par sa propre volonté, dans les limites du principe supérieur du droit, et conformément au but collectif qu'il est appelé à réaliser* » [(4)].

La notion de la souveraineté a été également définit par la constitution française de 1958 dans les articles suivants:

- L'article 2 qui définit les principaux symboles de la république et le principe de gouvernement de la République française ;

> **[Art 2 de la constitution de 1958]**
> *« La langue de la République est le français.*
> *L'emblème national est le drapeau tricolore, bleu, blanc, rouge.*
> *L'hymne national est la "Marseillaise".*
> *La devise de la République est "Liberté, Egalité, Fraternité".*
> *Son principe est : gouvernement du peuple, par le peuple et pour le peuple. »*

---

(1) A. PECHEUL, La souveraineté dans tous ses états, Edition Cujas, Paris, 2011.

(2) A. PECHEUL, La souveraineté dans tous ses états, Edition Cujas, Paris, 2011.

(3) J. BOUDIN, Six livres de la République, Fayard, 1986, P. 122.

(4) L. LE FOUR, État fédéral et confédération d'états, Marchal et Billard, 1986. P.443

- L'article 3 qui fait partie du titre I sur la souveraineté, et traite de l'exercice de la et traite de l'exercice de la souveraineté nationale.

  [Art 3 de la constitution de 1958]

  « La souveraineté nationale appartient au peuple qui l'exerce par ses représentants et par la voie du référendum.
  Aucune section du peuple ni aucun individu ne peut s'en attribuer l'exercice.
  Le suffrage peut être direct ou indirect dans les conditions prévues par la Constitution. Il est toujours universel, égal et secret.
  Sont électeurs, dans les conditions déterminées par la loi, tous les nationaux français majeurs des deux sexes, jouissant de leurs droits civils et politiques. »

- L'article 4 qui traite les rôles des partis et groupements politiques et du principe de démocratie.

  [Art 4 de la constitution de 1958]

  « Les partis et groupements politiques concourent à l'expression du suffrage. Ils se forment et exercent leur activité librement. Ils doivent respecter les principes de la souveraineté nationale et de la démocratie.
  Ils contribuent à la mise en œuvre du principe énoncé au second alinéa de l'article 1er dans les conditions déterminées par la loi.
  La loi garantit les expressions pluralistes des opinions et la participation équitable des partis et groupements politiques à la vie démocratique de la Nation.»

Au niveau européen, dont l'union est une communauté constituée des États souverains, le terme de la souveraineté renvoie à une forme de protectionnisme économique incitant les politiques à préconiser le développement d'une protection souveraine face aux pays émergents. Par contre, à l'intérieur de l'Union, la souveraineté européenne signifie que les États-membres transfèrent certains droits de décision aux institutions mises en place: Commission européenne, la banque centrale européenne, *etc*. Pour certains eurosceptiques, l'intégration européenne a considérablement réduit la souveraineté des États membres, alors que pour les pro-européens, l'intégration a plutôt renforcé la souveraineté des États membres. Pour ces derniers, la souveraineté a permis de construire les État-nations républicains et pluriels du monde moderne, elle a été la clé de l'intégration et de l'équilibre européen.

Cependant, Aux Royaume Unies, comme le précise Philippe Raynaud et Stéphane Rials[(1)], le terme de souveraineté (ou Sovereignty) se rapporte à un exercice absolutiste du pouvoir alors qu'aux États-Unis, la souveraineté se limite aux questions d'autorité et de contrôle comme l'affirme Stephen Krasner[(2)].

[(1)] P. RAYNAUD et S. RIALS, Dictionnaire de philosophie politique, Paris, PUF, 2003.

[(2)] S. KRASNER, Sovereignty: Organized Hypocrisy, Princeton University Press, 1999.

Au Maroc, l'article 2 de la constitution marocaine de 2011 définit la souveraineté en trois volets principaux :

> **[Article 2.1**]
> « *La souveraineté nationale appartient au peuple marocain dans son ensemble qui l'exerce par la désignation tous les cinq (5) ans, au suffrage universel direct et secret, de ses représentants au parlement et par voie de référendum pour la révision de la Constitution. Aucun individu ou groupement d'individus ni aucune personne morale ne peut s'en attribuer l'exercice*».
>
> **[Article 2.2]**
> *« Les partis politiques, les organisations syndicales, les collectivités territoriales et les Chambres professionnelles concourent à l'organisation et à la représentation des citoyens*.»
>
> **[Article 2.3]**
> «*Il ne peut y avoir de parti unique ni de media unique*.»

Ainsi, comme pour la France, la souveraineté au Maroc consiste à concentrer le pouvoir et la force de coercition dans l'État afin de défendre son intégrité territoriale (problème du Sahara dite « occidentale »), son indépendance à l'extérieur comme à l'intérieur. Il s'agit ici d'une expression collective des choix des citoyens sans subordination à une autorité étrangère. Les seules limitations de ces choix citoyens proviennent du droit international et des traités dont les traités européens.

c) Vers une cybersouveraineté

L'État moderne selon Etienne Wasmer et Marc Ferracci[(1)] doit utiliser les outils numériques qu'il possède afin de les mettre au service de sa propre efficacité. Un tel État doit se configurer autour des services numériques pour répondre aux nouvelles aspirations de ses citoyens. Au cœur de ces outils numérique ; le Cloud Computing, le Big data. Leurs nouveaux usages[(2)] représentent un grand défi pour les États et touchent à leurs souverainetés. En effet, le numérique soulève de nouveaux enjeux de souveraineté à la fois pour la création et pour l'application du droit sur le territoire national. Cette application est remise en question par le caractère dématérialisé et transfrontalier des nouveaux usages du numérique. Par conséquent, les modes traditionnels de régulation des pouvoirs sont désormais remis en question. Les pouvoirs publics sont menacés d'obsolescence dans leur capacité à encadrer le marché pour l'intérêt général ou encore à fournir des services publics garants de l'égalité pour tous les citoyens. D'ailleurs, les nombreuses questions autour de la taxation des entreprises de l'Internet et l'exploitation des données personnelles en est un simple exemple.

---

(1) E. WASMER et M. FERRACCI, État moderne, état efficace, Odile Jacob¸ 2011.

(2) Nous pouvons citer par exemple le stockage des données sensibles, la multiplication des objets connectés, croissance des services disponibles sur Internet, la traçabilité et la surveillance des usagers sur Internet, etc.

La souveraineté numérique fait encore l'objet de discussion et débats afin de définir ses conteneurs, les conditions et outils de son exercice ainsi que sa position par rapport à la souveraineté politique. En effet, dans son sens commun[(1)], l'expression de la souveraineté numérique, selon Pierre Bellanger, signifie «*la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques*»[(2)]. Le même auteur en donne une deuxième définition : «*Il n'y'a pas de souveraineté nationale sans souveraineté numérique. L'Internet est un réseau mondial sous contrôle des États-Unis. Les entreprises américaines y sont le plus souvent dominantes. La dépendance et le transfert de valeur occasionnés par ce déséquilibre doivent amener les pouvoirs publics à mettre en œuvre une politique industrielle de l'Internet*»[(3)].

Par la suite, les autorités publiques ont réapproprié l'utilisation du terme d'abord par Fleur Pellerin, ministre déléguée à l'économie numérique (2012-2014), qui indique «*vouloir défendre la souveraineté numérique de la France*»[(4)]. Puis par Axelle Lemaire, secrétaire d'État au numérique, en déclarant que «*de nouveaux acteurs doivent tenir un rôle dans la gestion d'Internet. La gouvernance est un enjeu politique au sens le plus noble du terme*.» [(5)]. Elle précise que les Européens « *ne doivent pas avoir un rôle passif* » en soulignant que le débat autour du numérique doit être porté à l'échelle européenne. Aussi, la députée socialiste des Côtes-d'Armor Corinne Erhe déclare que *« La souveraineté numérique, c'est être conscient des enjeux tout en étant capable de susciter des innovations, (…), la souveraineté, autrement-dit l'autorité et l'indépendance d'un État, implique de définir une stratégie lisible et de mettre en œuvre d'une politique industrielle forte* »[(6)]. De son côté, Didier Renard, président de Cloudwatt[(7)] opérateur de cloud souverain français, a déclaré à la même occasion que « *l'enjeu de la souveraineté numérique est à la fois celui de la reconquête, la sécurité nationale et la création nette d'emploi et de valeur* »[(8)].

---

(1) La notion de sens commun se désigne à une forme de connaissance regroupant les savoirs socialement transmis et largement diffusés dans pour un objet donnée.

(2) Une définition donnée par Pierre Bellenger son un article « De la souveraineté en général et de la souveraineté numérique en particulier » publié dans les Echos le 30 août. 2011. Article disponible sur le lien : http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm, dernière consultation 09/07/2015.

(3) Cette définition est donné par Pierre Bellenger pendant son audition dans le cadre des consultations du conseil national du numérique en 2011.

(4) Une déclaration faite dans une interview accordée le 28 novembre 2012 à L'Express sur la politique gouvernementale relative aux nouvelles technologies.

(5) Pendant son discours à l'inauguration des nouveaux locaux de l'Afnic (Association française pour le nommage Internet en coopération) le jeudi 6 novembre 2014.

(6) Déclaration pendant la première édition des Assises de la souveraineté numérique pilotée par l'agence Aromates et organisées à Paris le 13 mai 2014

(7) Voir le chapitre 3 Système Technique dans la partie Cloud Computing

(8) Idem. Déclaration pendant la première édition des Assises de la souveraineté numérique pilotée par l'agence Aromates et organisées à Paris le 13 mai 2014

Ces diverses définitions de la notion de la souveraineté numérique au sens commun consistent à appliquer les principes de la souveraineté, cités plus haut, au domaine numérique afin d'assurer la sécurité et l'intégrité de l'État. Cependant, elles ne permettent pas de couvrir tous les aspects d'une souveraineté politique. Nous estimons qu'une définition complète doit prendre en compte les éléments suivants :

- Le caractère transfrontalier du numérique qui remet en question l'application des droits nationaux. Par exemple, assurer une concurrence plus loyale, la question de la soumission au droit et la fiscalité. En effet, les entreprises d'Internet profitent des différences entre les pays notamment en Europe pour privilégier de flexibilité fiscales et de droits ;
- Soulever des problématiques de visibilité de la norme applicable et de compétence des tribunaux nationaux avec la superposition et la concurrence des droits nationaux, régionaux et internationaux.

L'objectif d'avoir une définition précise d'une souveraineté numérique est de préserver les composantes traditionnelles de la souveraineté politique d'un État. Par ailleurs, les grands acteurs d'Internet proclament des ambitions souveraines. Par exemple, Google réclame « *organiser les informations à l'échelle mondiale dans le but de les rendre accessibles et utiles à tous* » alors que Facebook souhaite « *connecter le monde entier*».

Ces entreprises de Cloud Computing maitrisent bien l'ensemble des composantes d'une souveraineté. En effet, ces acteurs possèdent:

- *Un territoire* : Les applications mises à disposition sont assimilées à un territoire;
- *Une population* : Les utilisateurs sont, eux également, assimilés à des citoyens de ces applications ;
- *Une monnaie* virtuelle comme les jetons Bitcoin utilisée entre citoyen pour accomplir des actes d'achat ;
- *Une constitution*: Toutes les plateformes ont une ligne de conduite à respecter via leurs conditions générales d'utilisation (CGU), ces dernières peuvent être assimilées à une vraie constitution.
- *Une police et un pouvoir de coercition*: Elles jouent un rôle clé dans le contrôle des contenus, d'accès à Internet, à l'information et au savoir, *etc*. Elles ont également la capacité à traiter des données personnelles des utilisateurs, à surveiller et à contrôler leurs comportements sur les réseaux. Ces activités sont l'image de ce qui fait les services de sécurités d'un État.

Ainsi, la souveraineté numérique renvoie vers une cybersouveraineté. Une nouvelle notion qu'il faudra interroger pour en définir les différents conteneurs.

d) Vers une politique numérique souveraine

Pour faire face aux tentatives d'espionnage et au transfert massif des données sensibles vers des acteurs étrangers qui constituent une atteinte à la souveraineté d'un État, plusieurs experts considèrent qu'une prise de conscience des pouvoirs publics est nécessaire pour établir une politique souveraine en matière du numérique afin d'assurer une souveraineté numérique en développant des alternatives nationales.

L'objectif d'une telle politique doit être de nature horizontale et vise à mettre en place des conditions propices à la compétitivité économique. Elle doit être également intégrée dans d'autres politiques telles que celles liées au commerce, à la recherche et à l'innovation, à l'emploi, à la protection de l'environnement et à la sécurité publique.

Une politique numérique bien élaborée ne doit pas se limiter à équipier les usagers par de matériels informatique, mais au contraire, elle doit adopter une approche tournée vers l'avenir dont le Cloud Computing et le Big data occupent une place stratégique. D'ailleurs, en suivant ce credo, et dans le cadre du programme de la nouvelle France Industrielle, le ministère de la finance et de l'économie numérique, avait lancé 34 plans stratégiques dont le plan Cloud Computing et le plan Big data. Nous y reviendrons dans la section 3 dédié aux politiques publiques en matière d'adoption de Cloud et de Big data.

Pour élaborer des politiques publiques efficaces en matière numérique, l'État devrait s'inspirer de l'univers américain qui bénéficie de plusieurs partenariats public-privé (PPP)[(1)]. L'État doit également rassembler tous les acteurs nationaux : laboratoires de recherches, entreprises privées, jeunes entreprises, autorités publiques, *etc*, autour d'un projet national à la fois complet, innovant et au service de la France.

Au Maroc, le gouvernement a fait appel au fournisseur Cloud américain Microsoft pour l'accompagner dans sa mise en place d'une stratégie Cloud. En effet, lors d'un sommet tenu à Rabat en décembre 2013, les autorités marocaines et les experts de Microsoft ont travaillé ensemble pour élaborer le schéma directeur de mise en place d'un Cloud souverain marocain. Suite à notre entretien avec le directeur Microsoft Maghreb, il nous a confirmé le souhait de Microsoft d'aider le Maroc dans sa démarche et ainsi confirmé la mise en place de ce Cloud souverain au Nord du pays. D'autres politiques publiques doivent suivre afin d'équiper l'administration marocaine par des outils lui permettant une autonomie face aux éditeurs étrangers.

[(1)] Le partenariat public-privé (PPP) est un mode de financement par lequel une autorité publique fait appel à des prestataires privés pour financer et gérer un équipement assurant ou contribuant au service public. Le partenaire privé reçoit en contrepartie un paiement du partenaire public et/ou des usagers du service qu'il gère. Ce mode de financement est présent dans de nombreux pays sous des formes variées. (Source Wikipédia).

C. Ré affirmer l'État de droit à l'ère de la sécurité nationale et du Cyber-État

a) Contexte

Comme nous venons de le voir, la cybersurveillance et le cyberspace constituent de sérieux enjeux pour la souveraineté et la cybersouveraineté de l'État. En effet, les nouvelles formes de communication et d'échanges facilitées par les outils numériques complexifient la tâche des autorités publiques en charge de la sécurité publique et de la sécurité nationale. Ainsi, dans un contexte de forte charge émotionnelle liée à des événements nationaux (attentats du 07 Janvier en France et le risque permanent d'attentat terroriste au Maroc), ainsi qu'un contexte international très instable, nous observons une tendance du renforcement des pouvoirs de l'administration centrale et à une minimisation du rôle du juge sous couvert d'un impératif d'urgence et d'efficacité.

Comme le recommande le Conseil National du Numérique dans son rapport Ambition Numérique remis au premier ministre dans l'optique de préparation d'une loi dédiée au numérique, la préservation de la sécurité publique ne se bâtie pas sur des régimes d'exception mais seulement avec une justice bien formée et bien outillée. Cette justice est nécessaire pour faire face à ces nouveaux enjeux sécuritaires qui prennent des nouvelles formes comme les cyberattaques et le cyberespionnage, *etc*. Cette justice aura la charge de garantir l'équilibre entre le maintien de la sécurité publique et le respect des libertés publiques et individuelles des citoyens.

L'État de droit doit être consolidé pour mieux appréhender les problématiques de sécurité dans un monde numérique. Cela se passe en renforçant de façon considérable les capacités d'action et les moyens de la justice ainsi que la mise en place d'un cadre légal de l'action des acteurs du renseignement avec des outils de contrôle juridiques et démocratiques dédiés.

En France, le contrôle des activités de renseignement est actuellement assuré par deux organes :

- La Commission nationale de contrôle des interceptions de sécurité (CNCIS)[(1)] est une autorité administrative indépendante qui a pour mission de garantir le secret des correspondances en s'assurant de la légalité des interceptions de sécurité mises en œuvre par les autorités administratives pour prévenir les atteintes aux intérêts fondamentaux de la nation. Elle est composée de trois membres – un magistrat qui la préside et deux parlementaires désignés par chacune des assemblées –, assistés de deux magistrats de l'ordre judiciaire. Elle émet un avis sur la légalité de l'interception autorisée au regard des cinq motifs légalement admis : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ;

- La Délégation Parlementaire au Renseignement (DPR)[2] est un organe commun à l'Assemblée nationale et au Sénat, composé de huit membres, quatre députés et quatre sénateurs. Elle assure un contrôle de nature très différente de celui exercé par la CNCIS : politique, ce contrôle ne porte pas sur l'opérationnel, la communication de tout élément relatif aux opérations en cours ou aux procédures et méthodes opérationnelles étant expressément interdite par la loi. Depuis sa modification par la loi de programmation militaire du 18 décembre 2013, celle-ci lui confère la mission d'exercer «le contrôle parlementaire de l'action du Gouvernement en matière de renseignement » et d'évaluer « la politique publique en ce domaine ».

Ainsi, une loi vient encadrer le travail de la CNCIS via la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications. Dans son article 3, il inscrit :

> **[Article 3]**
> *« Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des télécommunications ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. »*

Cependant, ce cadre juridique dans lequel s'inscrit l'intervention de la CNCIS, à savoir la loi du 10 juillet 1991 qui a été conçue pour encadrer l'interception du contenu des communications apparaît désormais inadapté face aux évolutions induites par le Cloud Computing et le Big data. Or, la diversification des technologies et l'internationalisation des acteurs de l'Internet viennent bouleverser le schéma sur lequel repose le régime juridique en vigueur. La loi de programmation militaire (PLM) adoptée en 2013, la loi anti-terrorisme adoptée en 2014 et la nouvelle loi relative au renseignement adoptée en 2015 viennent combler ce manque juridique

---

[1] La loi n° 91-646 du 10 juillet 1991 avait confié à la CNCIS le contrôle de l'interception des correspondances émises par voie de communications électroniques. Par la suit, la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme a ajouté le contrôle des demandes de communication des données de connexion conservées et traitées par les opérateurs, fournisseurs d'accès ou hébergeurs (y compris les données relatives à la localisation des équipements terminaux utilisés). La CNCIS est membre permanent de la Commission consultative dite « R 226 », créée par le décret n° 97-757 du 10 juillet 1997 et chargée d'émettre des avis sur les demandes de commercialisation, d'importation, d'acquisition, de détention ou d'emploi des matériels susceptibles de porter atteinte au secret des correspondances, autorisées par le Premier ministre.

[2] La DRP a été créée par La loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.

b) La loi de programmation militaire 2014-2019

Une Loi de Programmation Militaire, abrégée LPM, est une loi visant à établir une programmation pluriannuelle des dépenses de l'État en matière militaire. Les lois de programmation militaire ont des durées d'application de quatre, cinq ou six ans. Depuis 2003, les LPM couvrent des périodes de six ans.

En effet, la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale voie son budget avoisine les 190 milliards d'euros de crédits jusqu'en 2019, soit 31,4 milliards par an selon des affirmations du ministère de la Défense le 10 Juillet 2014.

Ce texte de LPM (2014-2019) met l'accent sur la modernisation des équipements de défense avec une priorité donnée au renseignement militaire en prévoyant le mise en service de trois satellites CERES[(1)] d'interception électronique à horizon 2020. Il inscrit également parmi ses priorités la lutte contre les attaques et la criminalité informatique. En effet, l'article 20 de la loi précise que le système d'autorisation administrative de collecte des données de connexions (factures téléphoniques détaillées, historique des visiteurs ou utilisateurs d'un site web, d'un hébergeur de vidéo, d'un service de courriel, *etc*.) et des interceptions de sécurité (les écoutes téléphoniques, ou « écoutes administratives ») sont opérées par les services de renseignement.

Ainsi, l'article 20 de la Loi de Programmation Militaire (LPM) 2014-2019 organise la généralisation d'une « *surveillance en temps réel* » des « *informations et documents traités et conservés dans les réseaux* » pour les impératifs de la défense et la sécurité nationale avec la participation des opérateurs de télécommunication et de fournisseur Cloud Computing.

La Loi de Programmation Militaire (LPM) 2014-2019 permet à certains ministères : sécurité intérieure et défense, mais aussi économie et budget, d'autoriser la surveillance en temps réel de tout citoyen pour la « prévention de la criminalité et de la délinquance organisées. En effet, l'article 20 de la loi définit le périmètre d'intervention comme suit :

En effet, cet article 20 prévoit de modifier le code de la sécurité intérieure en y ajoutant notamment :

> « ***Art. L. 246-1.*** *– Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des*

---

(1) CERES (Capacité de Renseignement Electromagnétique Spatiale) est un programme français de satellites militaires d'écoute électronique chargé de collecter du renseignement d'origine électromagnétique.

informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date des communications. »

« ***Article L. 241-2*** *- Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article L. 242-1, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1.* »

Ainsi, la collecte de ces informations pour les besoins définis par la loi se fera auprès des fournisseurs d'accès à Internet (FAI) mais aussi auprès des fournisseurs Cloud Computing nationaux. D'ailleurs, l'ensemble des fournisseurs d'accès Internet sont également des fournisseurs des applications Cloud Computing.

L'adoption de cette loi et précisément son article 20 manifeste une profonde crise d'un pouvoir politique n'hésitant plus à porter atteinte aux droits fondamentaux sous prétexte des impératifs de la défense et de la sécurité nationale. Les technologies Cloud Computing et de Big data ne font qu'augmenter les possibilités de surveillance en offrant aux autorités des moyens technologique comme la centralisation et l'accès aux bases de données, traçabilité des comportements, etc.

c) La loi anti-terrorisme

Le texte de loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme, promulguée le 13 novembre 2014 et publiée au Journal officiel du 14 novembre 2014, vise à renforcer la lutte contre le terrorisme et à prendre en compte les évolutions récentes des actes de terrorisme et plus précisément celles qui s'appuient sur des technologies numériques comme le Cloud Computing et le Big data.

Ainsi, la loi anti-terrorisme vient compléter l'arsenal judiciaire des autorités face aux risques de sécurité à l'ère de Cloud et de Big data. En effet, cette loi consiste à renforcer la lutte contre le terrorisme et à prendre en compte les évolutions récentes des actes de terrorisme et spécialement ses aspects technologiques. Le texte renforce la répression de l'apologie du terrorisme et de la provocation à des actes de terrorisme. Il permet le blocage administratif de sites internet faisant l'apologie du terrorisme ou y provoquant. La loi étend également à l'apologie du terrorisme des exigences imposées aux fournisseurs d'accès à internet (FAI) et aux fournisseurs Cloud, déjà

astreints depuis juin 2004 à lutter contre la propagation de la pédopornographie, les atteintes aux mineurs, la haine raciale ou l'apologie des crimes de guerre, etc.

Pour s'adapter aux nouvelles techniques de stockage des données, les enquêteurs pourront perquisitionner les solutions Cloud Computing comme la messagerie électronique sur téléphone par exemple. Ils auront également le droit d'intercepter les discussions sur les logiciels d'appels téléphoniques sur Internet.

Cependant, Si la lutte contre le terrorisme est légitime surtout dans un contexte internationale mouvementé avec des engagements de la France dans plusieurs fronts internationaux, elle ne peut justifier de légiférer en urgence sans lancer un débat national sur les libertés publiques et permettre à l'ensemble de la population : citoyen, experts, décideurs politiques, etc, de s'exprimer et éviter de mettre en place des lois avec de graves atteintes aux libertés fondamentales. C'est ainsi que Observatoire des libertés et du numérique (OLN) considère que l'expérience de ces lois appliquées dans le monde (en particulier aux États-Unis, qui s'en sont faits des parangons du *Patriot Act*), montre que celui-ci n'est pas devenu plus sûr avec ces méthodes.

d) La loi relative au renseignement

La loi n° 2015-912 du 24 juillet 2015 relative au renseignement a été adoptée après les attentats de Janvier 2015. Elle vise à donner un cadre légal aux activités des services de renseignement et précisément en faisant appel à des technologies numériques dont le Cloud Computing et les technologies Big data alors qu'un rapport[(1)] parlementaire rédigé en 2013 avait montré que les services de renseignement agissent sans base légale et en dehors de tout contrôle autre que hiérarchique.

Cette loi soumet la mise en œuvre des techniques de renseignement à une autorisation du Premier ministre, après avis d'une autorité administrative indépendante. Il s'agit de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR). Ainsi, le recours aux techniques de surveillance encadrées par la loi devra obéir à une procédure spécifique. En effet, les demandes écrites seront adressées au Premier ministre qui donnera ou non son accord après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR). Cette dernière succèdera à la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS). Ainsi la CNCTR est composée de magistrats, d'une personnalité qualifiée pour ses connaissances en matière de communications électroniques et de parlementaires[(2)].

---

(1) Rapport N° 1022, enregistré à la Présidence de l'Assemblée nationale le 14 mai 2013 par MM. JEAN-JACQUES URVOAS ET PATRICE VERCHÈRE autour de l'évaluation du cadre juridique applicable aux services de renseignement

(2) Un amendement adopté par l'Assemblée nationale porte la composition de cette autorité de 9 à 13 membres : 3 députés, 3 sénateurs, 3 membres du Conseil d'État, 3 magistrats de la Cour de cassation et un représentant de l'Autorité de régulation des communications électroniques et des postes (ARCEP)

Cependant, cette loi n'est pas un projet de loi de lutte « anti-terroriste » mais un projet loi sur le renseignement dont l'article [Art. L.811-3] définit les champs concernés :

- La sécurité nationale ;
- Les intérêts essentiels de la politique étrangère et de l'exécution des engagements européens et internationaux de la France ;
- Les intérêts économiques et scientifiques essentiels de la France ;
- La prévention du terrorisme ;
- La prévention de la reconstitution ou du maintien de groupements dissous en application de l'article L212-1 ;
- La prévention de la criminalité et de la délinquance organisées ;
- La prévention des violences collectives de nature à porter gravement atteinte à la paix publique ;

D'ailleurs, la lutte contre le terrorisme arrive en 4ème position, la sécurité nationale, elle, est en première position.

Ainsi, parmi les techniques de renseignements autorisées par la loi, on retrouve :

- les sondes (article L. 851-2)
- les « boîtes noires » (article L. 851-3)
- la géolocalisation d'une personne, d'une voiture ou d'un objet (article L. 851-5)
- l'utilisation d'IMSI Catcher (article L. 851-6)
- l'interception des correspondances (article L. 852-1)
- la sonorisation et la captation d'image dans des lieux privés (article L. 853-1)
- les keyloggers (article L. 853-2)

Cependant, l'article L. 811-4 du projet de loi donne compétence au gouvernement pour élargir à l'avenir le nombre de services relevant des ministres de la défense et de l'intérieur ainsi que des ministres chargés de l'économie, du budget ou des douanes qui peuvent recourir aux techniques de renseignement. Dans l'étude d'impact lié à ce projet, le gouvernement envisage de conférer à « certains services de police » des moyens en la matière. En effet, l'article L. 851-2 autorise dans le cadre de la prévention du terrorisme le recueil en temps réel des opérateurs des données de personnes « préalablement identifiées comme présentant une menace » en se basant sur des technologies Big data.

Les finalités de cette loi sur le renseignement sont légitimes. Certes donner un cadre légal aux activités des services de renseignement, qui fonctionnent jusqu'à présent dans un cadre illégale, est nécessaire pour le respect des droits fondamentaux des citoyens mais cette loi présente un certain nombre de points inquiétants, et précisément dans l'atteinte au respect des libertés individuelles. Entre-autres, cette loi permet de :

- Une légalisation massive des pratiques illégales des services de renseignement permettant une surveillance de masse ;

- Dispositions permettant la collecte généralisée des données des citoyens dans Le Cloud Computing et en se basant sur les technologies big data pour leurs traitement ;
- Extension des champs d'action du renseignement intérieur et extérieur, avec des finalités extrêmement vastes et floues.

Pendant le séminaire jeune de l'Institut des Hautes Etudes de Défense Nationale (93eséminaire Jeunes –Paris Ile de France), nous avons travaillé sur une analyse approfondie de cette loi. Nous avons pu confronter les différents points de vue dans un contexte chargé émotionnellement suite aux attentats de janvier 2015 et celle de novembre 2015.

e) Travaux du séminaire IHEDN - Jeunes –Paris Ile de France : La loi de renseignement du 24 juillet 2015

a. Introduction

Les opinions émises, les analyses proposées par les auteurs de ce rapport, n'engagent pas l'IHEDN

La question des libertés individuelles a toujours occupé une place dominante dans les esprits, Montesquieu disait d'ailleurs « la liberté ne s'obtient que par des coups d'éclats, mais se perd par une force insensible ». A la suite de l'adoption de la loi 24 juillet 2015, la question des libertés individuelles est au cœur du débat public. Celle-ci englobe notamment le droit à la sûreté, le droit d'aller et venir, le droit à la vie privée. Ces principes rentrent dans la catégorie des libertés individuelles, elles-mêmes ayant trait à la sécurité publique. En vertu de sa fonction régalienne, l'Etat se doit de garantir la sécurité publique, au risque de porter atteinte aux libertés individuelles. Ce dilemme est la volonté de rechercher un juste milieu entre la préservation des libertés individuelles et la sécurité collective. L'instabilité du contexte complexifie pourtant cette recherche d'équilibre.

La loi du 24 juillet 2015 renforce les dispositions relatives à la lutte antiterroriste, édictées par la loi du 13 novembre 2014 qui tend à légitimer des mesures portant atteinte aux libertés individuelles. La loi dispose :

- une légalisation de pratiques de surveillance de la part des services de renseignement envers les citoyens français, pratiques liberticides mais constitutionnellement validées.
- la subordination de ces pratiques à l'avis consultatif d'une Commission de contrôle.

Ce constat amène à l'interrogation suivante : En quoi la loi du 24 juillet 2015, législation circonstancielle, peut-elle générer un déséquilibre dans l'arbitrage entre sécurité publique et libertés individuelles ?

Dans le contexte actuel, la crainte liée au terrorisme modifie le rapport des citoyens à la sécurité. Parallèlement, on constate la non transparence des activités de renseignement, sous la direction de l'administration et en l'absence de tout réel encadrement.

Dans ce cadre, la loi sur le renseignement se veut protectrice des libertés individuelles. Son objectif étant une meilleure acceptation par l'opinion publique des méthodes utilisées par les renseignements dans la lutte contre le terrorisme, face à une demande sécuritaire. Mais, le contexte de cette loi en a favorisé son acceptation populaire et médiatique, sans réelle connaissance de son contenu.

b. Scénario 1 - Une applicabilité technique incertaine

i. Hypothèse:

Cette loi est techniquement inefficace du fait d'un manque de moyens humains et financiers. L'application de l'Etat d'urgence a empêché son évaluation.

Constat sur les possibilités offertes aux renseignements par la Loi:

- Un flux d'informations trop important ne peut être traité de façon efficace: un algorithme avec une fiabilité de 99 % identifierait jusqu'à 600 000 suspects par erreur et donc abandon de certains suspects, soupçonnés de radicalisme, alors qu'il y a focus sur d'autres.
- Les boites noires promises ne sont pas actuellement fonctionnelles ;
- La loi n'a pas encore été traduite dans les faits, faute de délai nécessaire à son application. Aucun moyen permettant la collecte de renseignement, tels que les boites noires, n'a pu être mis en place, à ce jour.

ii. Objectif:

Donner aux services de renseignement les moyens pratiques d'appliquer cette loi.

Recommandations
- Augmenter des effectifs des services de renseignement - Augmenter des ressources financières - Privilégier la qualité à la quantité d'informations récoltées dans un objectif d'efficacité

Avantages	Inconvénients
- Meilleur gestion des données. - Accroissement de la performance des mesures de la loi. - Augmentation de la précision des filtres, pour un meilleur suivi des suspects.	- Engrangement des dépenses importantes. - Augmentation du budget nécessaire à l'application des mesures se fera au détriment d'autres secteurs. - Risque de passer à côté de suspects.

c. Scénario 2 – Des moyens démocratiques au service de l'optimisation de la loi

i. Hypothèse :

L'adoption de la loi sur le renseignement via une procédure législative accélérée a court-circuité son acceptation par la population rompant le contrat social liant l'État à ses citoyens.

ii. Constat :

Articles et sondages montrent que l'acceptation de la loi a été préalablement et largement contestée par la société civile:

- Instrumentalisation des sondages en faveur de la loi
  - Omission du fait que "76% des français ne sont pas d'accord avec les mesures mises en place pour aboutir à "plus de sécurité" (juillet 2015)
  - Certes, le "16 Juillet 2015 - 69% des français trouvent la loi 'utile' ", mais "seuls ⅓ des français avouent avoir bien compris de quoi il s'agit."
- Manque de transparence - le 13 avril 2015, "63% des français sont favorables à la limitation des libertés individuelles pour lutter contre le terrorisme"
- Omission des mises en garde - Amnesty, la CEDH, Transparency International et même l'ONU avaient publié plusieurs rapports sur le fait que ces nouvelles "mesures de surveillance désormais autorisées sont complètement disproportionnées"

iii. Objectif :

Rétablir le contrat social en mettant en place un système démocratique hybride où le citoyen reprend une place centrale dans le processus d'adoption et de contrôle de la loi.

Recommandations
- Mettre en place des dispositifs de démocratie participative : référendum. - Mettre en place des contre-pouvoirs afin de permettre à la société civile de s'investir : participation des citoyens - Transparence de l'État sur les motifs et le contenu de la loi : définir les contours de la loi.

Avantages	Inconvénients
- Un meilleur engagement du citoyen – le citoyen devient acteur et non plus spectateur. - Une simplification du jargon juridique - La possibilité de juger de la satisfaction de la population.	- Commission plus nombreuse = plus de lourdeur et complexité. - Référendum = processus long et coûteux. - Question trop protéiforme pour être soumise a un « oui vs. non ». - Risque d'utilisation abusive des numéros verts. - Risques de fuites des données classifiées vers le domaine public.

d. Scénario 3 : Des moyens juridiques au service de l'optimisation de la loi

i. Hypothèse :

Un recueil accru de renseignements, dans des situations futures de plus en plus graves, remettrait en cause la proportionnalité entre sécurité et libertés individuelles. Celle-ci est en effet dépendante d'un contrôle des mesures restrictives aux libertés par le juge judiciaire, absent en l'espèce.

ii. Constat:

A terme, la menace terroriste risque en effet de s'amplifier. De fait, la collecte accrue de données par les services de renseignement va se faire sentir. Or, les citoyens ne pourront continuer à se reposer sur cette loi pour préserver leurs libertés individuelles, car celle-ci introduit un déséquilibre entre les pouvoirs administratifs et judiciaires qui dessert la protection des libertés individuelles.

iii. Objectif :

Un objectif de préservation de l'Etat de droit : contre-pouvoirs, séparation des pouvoirs pour un meilleur contrôle de l'atteinte aux libertés individuelles tout en conservant un niveau de sécurité satisfaisant.

Recommandations	
Renforcer le pouvoir de la commission	Donner le pouvoir à la Commission de rendre un avis conforme préalable (ie. contraignant) pour les services de renseignement. - Garantir une consultation **obligatoire** de la commission *a priori* - Restreindre et définir les conditions permettant au 1er ministre de contourner cet avis. - nécessité d'intelligibilité et de clarté de la loi (Objectif à Valeur constitutionnelle + protéger par la Convention Européenne des Droits de l'Homme) - Modifier la composition de la commission pour une meilleure indépendance et impartialité et éviter les atteintes disproportionnées aux libertés individuelles: plus de membres du judiciaire
Donner plus de pouvoir au juge judiciaire = garant de l'atteinte aux libertés individuelles	- Un contrôle dès le début de la procédure. - Consultation préalable et jugement conforme. - Donner une compétence à la cour de cassation et non au Conseil d'Etat dans le contrôle à posteriori.

Avantages	Inconvénients
- Renforcement de la séparation et du contrôle des pouvoirs - Renforcement de la protection des libertés individuelles, comme affirmé initialement par la loi - Renforcement de la légitimité de l'action des services de renseignement (Vis à vis de l'Opinion Publique) - Renforcement de l'effectivité et efficacité de la Loi et de la protection - Solution effective et institutionnelle - plus que circonstancielle et émotionnelle	- Multiplicité des acteurs et des interfaces (fuites? perte d'information? Secret défense? Présomption d'innocence?) - Quid des ressources ? Financières? Humaine? En terme de compétence? - Lourdeur administrative - Complexification

e. Conclusion générale

Une loi sur le renseignement efficace doit s'inscrire dans une logique structurelle et institutionnelle pérenne, maximisant la sécurité publique, tout en en garantissant les libertés individuelles. Les moyens d'application d'une telle loi se doivent d'être clairement définis, répartis judicieusement entre les différentes autorités compétentes et placés sous le contrôle de contre-pouvoirs renforçant sa légitimité. C'est dans cette optique qu'un rééquilibrage entre pouvoir Administratif et Judiciaire dans la loi actuelle s'impose. Cet équilibre se matérialiserait par un passage obligatoire devant la commission de contrôle ou devant un juge judiciaire, dont les avis seraient contraignants.

f. Liste des participants :

- Helene TREHIN : Collège de Défense de l'OTAN
- Edouard GHEERBRANT : Archery Strategy Consulting
- Alexandre PINHAS : Dassault Aviation
- Myriam ALLAIN : M2. Université Paris 1 Panthéon-Sorbonne
- Raphael AGENEAU : Brigade Sapeurs-Pompiers de Paris
- Marine DE FONTANGES : M2. UVSQ en alternance
- Aldric DE LA CROIX :L3 Université Jean Moulin Lyon III
- Constance DUPUIS : L2 Institut Catholique de Paris
- Said EL OUAZZANI : Accenture consulting
- Marie-Camille GAINCHE : M2. IRCOM
- Gaspard LE ROUX : M1. Sciences Po Lille
- Anastasia PAROUTY : M1. Université Paris 1 Sorbonne
- Antoine SAOUT : Armée de l'Air
- Julien TYBALAN : Stagiaire en formation professionnelle – e2c78

g. Bibliographie de l'analyse

i. Conférencier et publication:

- Madame Moliner-Dubost, maître de conférences à l'Université Lyon III
- Wanda MASTOR, « La loi sur le renseignement du 24 juillet 2015: La France, Etat de surveillance? », Actualité Juridique, Droit Administratif (AJDA), 2015.

ii. Loi, décret, textes officiels :

- Assemblée Générale des Nations Unies, Déclaration Universelle des Droits de l'Homme, résolution, 1948.
- Conseil de l'Europe, Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 4 nov. 1950, entrée en vigueur le 3 sept. 1953.

- C.C., 23 juillet 2015, n°2015-713 DC, Loi sur le renseignement.
- DEBRE Michel, Constitution de la cinquième République, 1958, Paris.
- Rapport d'Amnesty International. http://www.amnesty.fr/Nos-campagnes/Liberte-expressio n/Actualites/Loi-renseignement-un-grand-coup-aux-droits-humains-15714 . Consulté le 22/02/16.

iii. Sitographie :

- Site Atlantico. http://www.atlantico.fr/decryptage/63 -francais-favorables-limita tion-libertes -individuelles-pour-lutter-contre-terrorisme-yves-marie-cann-2089085.html. Consulté le 24/02/16.
- Site de l'Assemblée Nationale. http://www.assemblee-nationale .fr/14 /dossiers / rensei gnement.asp. Consulté le 23/02/16.
- Site LégiFrance. https://www.legifrance.gouv.fr/affich Texte.do?cidTexte =JORFTEX T000030931899&categorieLien=id. Consulté le 22/02/16.
- Site Le Monde. http://www.lemonde. fr/pixels/article/ 2016/02/15/loi-sur -le-renseignement -les-boites-noires-loin-d-etre-mises-en-place_4865698_4408996.html. Consulté le 23/02/16.
- Site Le Monde. http://www.lemonde.fr/pixels/article/2015/03/18/les-critiques-de-la-cnil-contre-le-projet-de-loi-sur-le-renseignement_4595839_4408996.html. Consulté le 23/02/16.
- Site le Monde. http://www.lemonde.fr/pixels/article/2015/05/06/loi-renseignement-des-dizaines-de-milliers-de-personnes-vont-etre-suspectees-a-tort_4628392_4408996.html. Consulté le 23/02/16.
- Site du Sénat. http://www.senat.fr/rap/r15-036/r15-036_mono.html#toc22. Consulté le 22/02/16

f) De la Sécurité nationale comme doctrine de l'État

Sur le plan chronologique, le concept de sécurité nationale a été employé dans le cadre des télécommunications en 1991 dans l'article 3 de la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications :

> **[Art. 3]**
> « *Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des télécommunications ayant pour objet de rechercher des renseignements intéressant* ***la sécurité nationale****, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées*».

Dans sa version actualisée de 2013 :

> **[L241-2]**
> Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article L. 242-1, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant **la *sécurité nationale***, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1[(1)].

L'ancien président de la république Nicolas Sarkozy avait déclaré dans sa préface du livre blanc 2008: « *Le Livre Blanc de 2008 acte la fin du clivage traditionnel entre sécurité intérieure et sécurité extérieure. Il dépasse le cadre strict des questions de défense. Il élargit la réflexion à une sécurité nationale qui intègre désormais des dimensions importantes de la politique de sécurité intérieure* ». Le concept de Sécurité Nationale sera entériné et repris par le Livre Blanc de 2013.

[(1)] Code de la sécurité intérieure TITRE IV : INTERCEPTIONS DE SÉCURITÉ. Chapitre Ier (version juin 2013).

> « *De ce travail émerge un nouveau concept ; celui d'une stratégie de* ***sécurité nationale*** *qui associe […], la politique de défense, la politique de sécurité intérieure, la politique étrangère et la politique économique. Cette stratégie porte une ambition européenne et internationale qui est au cœur de la vocation de la France dans le monde*».

Ainsi, dans le cadre de la LPM (2014-2019), nous avons recensé 26 utilisations de la notion de la sécurité nationale. En effet, comme en témoigne ce changement de titre dans son article 2 du préambule: « *Une nouvelle stratégie de défense et de sécurité nationale* » est remplacé par le titre suivant : « *Une stratégie de défense et de* ***sécurité nationale confortée***»

Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure n°2 (LOPPSI 2) (rectificative 2011) pour la période 2009-2011 :

> **[Art. L. 1142-2]**
> « *Le ministre de l'intérieur est responsable de la préparation et de l'exécution des politiques de sécurité intérieure et de sécurité civile qui concourent à la défense et à la* ***sécurité nationale*** *et, il est, à ce titre, sur le territoire de la République, responsable de l'ordre public, de la protection des personnes et des biens ainsi que de la sauvegarde des installations et ressources d'intérêt général. /.../* »

Pour situer l'emploi du concept de sécurité nationale dans le cadre français en suivant les normes internationales et européennes, nous avons :

- La convention européenne des Droits de l'Homme et des Liberté fondamentales Convention de Genève de 1951 relative au statut des réfugiés[(1)]:

> **[Art 9.]**
> *« Aucune des dispositions de la présente Convention n'a pour effet d'empêcher un État Contractant, en temps de guerre ou dans d'autres circonstances graves et exceptionnelles, de prendre provisoirement, à l'égard d'une personne déterminée, les mesures que cet État estime indispensables à la sécurité nationale, en attendant qu'il soit établi par ledit État Contractant que cette personne est effectivement un réfugié et que le maintien desdites mesures est nécessaire à son égard dans l'intérêt de sa* ***sécurité nationale****. »*
>
> **[Art 28]**
> « *Les États Contractants délivreront aux réfugiés résidant régulièrement sur leur territoire, des titres de voyage destinés à leur permettre de voyager hors de ce territoire à moins que des raisons impérieuses de* ***sécurité nationale*** *ou d'ordre public ne s'y opposent ; les dispositions de l'Annexe à cette Convention s'appliqueront à ces documents. Les États Contractants pourront délivrer un tel titre de voyage à tout autre réfugié se trouvant sur leur territoire ; ils accorderont une attention particulière aux cas de réfugiés se trouvant sur leur territoire et qui ne sont pas en mesure d'obtenir un titre de voyage du pays de leur résidence régulière. »*

[(1)] Convention et protocole relatif au statut des réfugiés, Article 9, Article 28 et article 32.

[Art 32]

«*Les États Contractants n'expulseront un réfugié se trouvant régulièrement sur leur territoire que pour des raisons de sécurité nationale ou d'ordre public.*

L'expulsion de ce réfugié n'aura lieu qu'en exécution d'une décision rendue conformément à la procédure prévue par la loi. Le réfugié devra, sauf si des raisons impérieuses de ***sécurité nationale*** *s'y opposent, être admis à fournir des preuves tendant à le disculper, à présenter un recours et à se faire représenter à cet effet devant une autorité compétente ou devant une ou plusieurs personnes spécialement désignées par l'autorité compétente. Les États Contractants accorderont à un tel réfugié un délai raisonnable pour lui permettre de chercher à se faire admettre régulièrement dans un autre pays. Les États Contractants peuvent appliquer, pendant ce délai, telle mesure d'ordre interne qu'ils jugeront opportune* ».

- La convention européenne des Droits de l'Homme et des Liberté fondamentales (1950):

[Art 6]

« Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. Le jugement doit être rendu publiquement, mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la ***sécurité nationale*** *dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice »*.

[Art 8]

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la ***sécurité nationale****, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

[Art 10]

« Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations. L'exercice de

ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la ***sécurité nationale****, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire* ».

[Art 11]

« *Toute personne a droit à la liberté de réunion pacifique et à la liberté d'association, y compris le droit de fonder avec d'autres des syndicats et de s'affilier à des syndicats pour la défense de ses intérêts. L'exercice de ces droits ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la* ***sécurité nationale****, à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. Le présent article n'interdit pas que des restrictions légitimes soient imposées à l'exercice de ces droits par les membres des forces armées, de la police ou de l'administration de l'État*».

Pour Gabriel Péries[(1)], la notion de la sécurité nationale est loin d'être neutre et s'interroge sur le contenu de cette notion. Il souligne que la jurisprudence renvoie à la Convention européenne de sauvegarde des Droits de l'Homme de 1950, qui pose dans son article 8, relatif au respect à la vie privée, des limites et qui stimule que *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence […] est nécessaire à la sécurité nationale, […].* ».

Marc-Antoine Granger souligne que « *la sécurité nationale doit- elle être considérée comme un objectif de sauvegarde de l'ordre public ? Dans le silence du Conseil, une telle interprétation est trop hasardeuse. Tout bien pesé, l'explication de l'occurrence est décevante au sens où le juge constitutionnel s'y est, semble- t-il, référé moins par nécessité que par facilité. Le Conseil ne paraît pas avoir « théorisé » l'usage de ces termes et s'est abstenu de penser sa relation avec l'objectif de sauvegarde de l'ordre public. Sans doute par commodité, il s'est contenté de reprendre les termes usités par le législateur* » [(2)]. Les propos de Granger montrent que le concept de la Sécurité Nationale est flou et reste une doctrine au contenu indéterminé.
A partir de ces éléments émergent un nouveau concept celui d'une stratégie de sécurité nationale[(3)]. En effet, cette stratégie de sécurité est une association de plusieurs politiques publiques:

- La politique de défense qui permet d'assurer la sécurité de la nation face aux risques d'agression armée, le respect de nos engagements internationaux en matière de défense, la contribution de la France au maintien de la paix et de la sécurité internationale, la participation à la protection de la population sur le territoire en appui des dispositifs de sécurité intérieure et de sécurité civile, et à l'étranger ;
- La politique de sécurité intérieure qui permet d'assurer de façon permanente la protection de la population, garantir le fonctionnement régulier des pouvoirs publics et le maintien de la vie normale du pays en cas de crise, et défendre les intérêts de sécurité de la nation contre toute menace non militaire susceptible d'y porter atteinte ;
- D'autres politiques publiques, en premier lieu la politique étrangère et la politique économique, qui contribuent directement à la sécurité nationale.

---

(1) G. PERIES, La confiance au prisme de la « sécurité nationale». Une analyse critique à l'ère des réseaux numériques, Politiques sécuritaire et surveillance numérique, P-A CHARDEL (Coord), Paris, Hermès, 2014, P.59.

(2) M-A GRANGER, Constitution et sécurité intérieure. Essais de modélisation juridique, LGDJ, 2011, p. 83-84.

(3) LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. Disponible pour consultation sur l'URL *http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825. Dernière consultation le 02 Juillet 2015 à 18h.*

Les objectifs de la stratégie de sécurité nationale sont définis par l'article L.1111-1 du code de la Défense, qui stimule que :

> **[Art L.1111-1]**
> « *Identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter. L'ensemble des politiques publiques concourt à la Sécurité nationale. La politique de Défense a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées. Elle contribue à la lutte contre les autres menaces susceptibles de mettre en cause la Sécurité nationale. Elle pourvoit au respect des alliances, des traités et des accords internationaux et participe, dans le cadre des traités européens en vigueur, à la politique européenne de sécurité et de défense commune*. »[(1)]

Cependant, comme le souligne Gabriel Péries[(2)], la loi de programmation militaire (LPM) pour la période 2009-2014 dans son Chapitre II intitulé : « *Organisation des pouvoirs publics dans les domaines de la défense et de la sécurité nationale* », précise dans son art. 5 que l'ancien art 1111-1 du Code de la Défense est remplacé par des « nouvelles dispositions», où il est inscrit que, dorénavant *« l'ensemble des politiques publiques concourt à la sécurité nationale*» (nouvel art L. 1111-1) ; et intronise l'indistinction entre affaires intérieures et extérieures :

> **Art. L. 1142-2**.
> **«** *Le ministre de l'Intérieur est responsable de la préparation et de l'exécution des politiques de sécurité intérieure et de sécurité civile qui concourent à la défense et à la sécurité nationale et, il est, à ce titre, sur le territoire de la République, responsable de l'ordre public, de la protection des personnes et des biens ainsi que de la sauvegarde des installations et ressources d'intérêt général.* »[(3)]

Au final, quel que soit le texte juridique consulté, la notion de sécurité nationale est restrictive des libertés publiques et individuelles plus précisément dans La LPM (2009-2014) et dans la LOPSI II. Ainsi en aucun moment, le contenu de cette notion de sécurité nationale n'est défini. Il reste donc à la discrétion des autorités publiques.

---

(1) L'article « L1111-1 » disponible sur le site Legifrance, dernière consultation 24 juin 2015 à 16h40.

(2) G. PERIES, La confiance au prisme de la « sécurité nationale». Une analyse critique à l'ère des réseaux numériques, Politiques sécuritaire et surveillance numérique, P-A CHARDEL (Coord), Paris, Hermès, 2014, P.59.

(3) Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. Disponible pour consultation sur l'URL http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825. Dernière consultation le 02 Juillet 2015 à 18h.

Toutefois, pour protéger les acquis en terme de libertés individuelles et collectives ainsi restaurer un climat de confiance dans un État de droit, il est important d'adopter certaines règles afin d'encadrer les activités de surveillance des services de renseignement. Cet axe a été largement débattu dans la cadre de la concertation nationale[(1)] pour le numérique, demandée par le premier ministre. Cette concertation coïncidait d'ailleurs avec les attentats de Janvier 2015. Nous reprenons ci-dessous certaines recommandations publiées dans le rapport final soumis au premier ministre et qui fera base de préparation de projet de loi lié au numérique. Il s'agit donc de :

- ***Recommandation 1****:*

Mettre en place cadre légal du renseignement qui permet d'allier efficacité et respect des libertés publiques et individuelles. Pour y arriver, le conseil national du numérique insiste sur la nécessité de :

- Introduire au plus haut niveau de la hiérarchie des normes un principe selon lequel la surveillance de masse, généralisée et indifférenciée, est étrangère à l'État de droit ;
- Proscrire le recours à une gouvernance algorithmique de la surveillance. Le projet de loi sur le renseignement introduit une détection automatisée des "signaux faibles" liés à une menace terroriste. Ce modèle suppose une surveillance préalable indiscriminée des métadonnées (données de connexion) et confine à une forme de surveillance de masse. Si une limitation qualitative du dispositif s'avère impossible, il conviendrait de renoncer à ces techniques, dont l'installation dans les réseaux (infrastructures, Cloud, etc.) est coûteuse pour en terme de budgets comme pour les libertés. L'efficacité d'une surveillance de masse des métadonnées est en outre particulièrement remise en cause aux États-Unis ;
- Définir plus strictement les finalités générales de recours à la surveillance et encadrer par la loi les missions de chacun des services de renseignement, aujourd'hui prévues par décret. Une formulation large des motifs du renseignement ne peut constituer le prétexte à une extension du champ de la surveillance ;
- Protéger les lanceurs d'alertes à l'image de Snowden. En effet, Le conseil National Souligne l'importance d'établir un régime français de protection des lanceurs d'alerte complet, plus clair et plus effectif ;

---

(1) Le Premier ministre Manuel Valls, en présence de Thierry Mandon, secrétaire d'Etat à la réforme de l'Etat et à la Simplification et d'Axelle Lemaire, secrétaire d'Etat au Numérique a donné samedi 4 octobre 2014 le coup d'envoi de la concertation nationale sur le numérique portée par le Conseil national du numérique (*CNNum*). Elle a pour objectif de faire émerger une vision partagée de la République numérique qui sera inscrite dans le projet de loi numérique en 2015.

- Doter le Défenseur des droits de la compétence nécessaire pour assurer une protection effective des lanceurs d'alerte. Pour les activités de renseignement touchant au secret défense, doter la CNCIS ou future CNCTR d'un pouvoir d'écoute, de réception des signalements et de médiation sur le sujet. Homogénéiser les protections aujourd'hui disparates pour qu'elles couvrent l'ensemble des problématiques (santé, fiscalité, renseignement, etc.) et cesser l'approche par silos thématiques ;
- Doter le Défenseur des droits de la compétence nécessaire pour assurer une protection effective des lanceurs d'alerte.
- Pour les activités de renseignement touchant au secret défense, doter la CNCIS ou future CNCTR d'un pouvoir d'écoute, de réception des signalements et de médiation sur le sujet.

- ***Recommandation 2*** *:*

Réformer le Fichier national des empreintes digitales et le Fichier national des empreintes génétiques.

- ***Recommandation 3*** *:*

S'engager contre l'exportation de technologies de surveillance et de censure d'Internet à destination des régimes autoritaires.

3. Chapitre 3 : Cybergéopolitique à l'ère du Cyber-État

A travers cette section, nous essayons d'étudier les effets de la géopolitique d'Internet et la cybergéopolitique sur le fonctionnement du Cyber-État et les relations internationales. Les relations internationales étaient une de nos théories mobilisées pour ce travail de recherche (*Cf. théories mobilisées dans l'Introduction*), dans le cadre d'une compréhension des transformations des instruments des politiques publiques consécutives à la révolution cybernétique.

Cette section traite des points principaux suivants :

- *Gouvernance d'Internet* : A travers cette partie, nous essayons de définir le concept de la *gouvernance* et son application sur Internet. Nous évoquerons les enjeux associés à la mise en place d'une gouvernance d'Internet à l'échelle mondiale afin de préserver son avenir. Nous analyserons également la mise en place des institutions internationales en charge d'assurer cette gouvernance. Nous ferons principalement références= aux travaux de Milton Mueller[(1)] et Lawrence Solum[(2)].

- *Instances mondiales ou « la république des ingénieurs »*: A travers cette partie, nous analyserons l'ensemble des institutions, si ce n'est certaines des composantes essentielles du champ institutionnel spécifique, qui opèrent pour une gouvernance d'Internet et qui permettent d'assurer techniquement son développement. Nous expliquerons également les procédures d'évolution des protocoles et la gestion de l'infrastructure technique Internet dans son sens large ;

- *Les rapports du pouvoir dans la gouvernance Internet* : Nous essayons ici de présenter les enjeux futurs de l'Internet d'aujourd'hui : entre la concurrence des plateformes, l'investissement dans les infrastructures, la gestion des instances de gouvernance, le partage des bénéfices, la taxation des activités, *etc*. Tous ces paramètres risquent de remettre en cause à tout moment le fonctionnement actuel d'Internet ;

- *Concept de neutralité du Net* : Nous présenterons dans cette partie le concept de la neutralité du Net. Nous essayerons de donner des définitions précises, d'analyser les enjeux et les motivations associés ainsi que le rôle des pouvoirs publics dans l'encadrement des activités liées à Internet ;

---

(1) M. MUELLER, Networks and stats: The global politics of Internet governance, MIT Press, 2010.

(2) L. SOLUM, Models Of Internet governance, In Bygrave, L et Bing J 5Eds), Internet Governance: Infrastructure and Institution, 2009.

A. La gouvernance d'Internet à l'ère du Cyber-État

Internet est devenu indispensable dans nos sociétés contemporaines qu'il était normal qu'il devînt un enjeu majeur des relations internationales et de la scène géopolitique à l'ère des technologies du Cloud Computing et du Big data.

En effet, la tension croissante autour de sa gouvernance s'accentue entre un réseau conçu techniquement sans frontières et un système international reposant sur la souveraineté politique des États avec une juridiction géographiquement définie. Les débats récents sur la gouvernance d'Internet et le rôle que doivent y jouer les États sont susceptibles de déclencher une nouvelle guerre froide entre les différents acteurs : Les États-Unis, l'Europe, Les pays de BRICS, Israël, l'Iran, et beaucoup d'autres nations. Le Maroc, quant à lui, s'aligne à la position européenne à travers les accords du groupe G29 et l'association de la francophonie pour la protection des données.

Pour comprendre ces tensions autour de la gouvernance d'Internet, il est important de prendre en compte la structure technique d'Internet. En effet, la gestion du protocole Internet comme le TCP/IP[(1)] relève de la responsabilité de l'organisation mondiale *Internet Engineering Task Force* (IETF). Les standards du Web sont gérés par l'organisation *World Wide Web Consortium* (W3C), les adresses d'Internet IP et les noms de domaines permettant à Internet de fonctionner à l'échelle mondiale sont gérés par l'organisation mondiale *l'Internet Corporation for Assigned Names and Numbers* (ICANN) sous contrôle des États-Unis. Ainsi, toutes ces organisations forment une structure difficile à gérer et dont les rapports de force entre acteurs sont omniprésents.

Le contrôle d'une telle structure technique et les enjeux cybergéopolitiques associés ont été largement débattus par 174 pays, dont la France et le Maroc, au sein du Sommet Mondial sur la Société de l'Information (SMSI)[(2)] pendant quatre années (2002-2005) de négociations intenses. Ces négociations ont donné naissance au Forum multipartenaire sur la gouvernance de l'Internet. Un forum annuel qui permet aux organismes internationaux, gouvernements, experts et organisations de la société civile de discuter sur un pied d'égalité du développement de l'Internet et d'autres domaines de politiques publiques étroitement lié à la gestion du réseau des réseaux : Internet.

---

(1) Nous reviendrons dans ce chapitre pour expliquer ces différentes éléments techniques liés à Internet : TCP/IP, W3C, IETF, DNS, *etc.*

(2) Le Sommet mondial sur la société de l'information (SMSI) s'est déroulé en 2 phases. La première phase, accueillie par le Gouvernement suisse, a eu lieu à Genève du 10 au 12 décembre 2003 et la deuxième phase, accueillie par le Gouvernement tunisien, a eu lieu à Tunis du 16 au 18 novembre 2005

Ce Forum sur la Gouvernance de l'Internet (FGI) est placé sous l'égide de l'Union Internationale des Télécommunications (UIT) qui lui-même rattachée à l'Organisation des Nations Unies (ONU).

Ainsi, lors de son dernier sommet, le *Netmundial*[(1)], qui a eu lieu en avril 2014 à São Paulo au Brésil, suite aux révélations par Snowden des affaires d'espionnage de la Présidente brésilienne Dilma Rousseff et de la Chancelière Allemande Angela Merkel, les différents pays, dont les États-Unis, ont discuté les multiples enjeux d'ordre économique mais également cybergéopolitique liés à l'Internet pour réduire à la domination américaine et éviter d'autres affaires d'espionnage économique et politique. Ainsi, comme le souligne Fayon:

> « *L'enjeu majeur d'aujourd'hui pour la gouvernance d'Internet est de savoir si l'on veut que le réseaux des réseaux soit utilisé comme un instrument exceptionnel de partage des connaissances, ou comme une arme géopolitique détenue par une superpuissance qui n'envisage guère d'en partager le contrôle, se réservant le droit de maintenir et de renvoyer ses adversaires, dans l'âge pré-Internet, c'est-à-dire, la préhistoire de la société de l'information*. »[(2)].

Cette rencontre de São Paulo s'inscrit dans la suite des autres rencontres internationales qui se sont tenues à Athènes en 2006, à Rio en 2007, à Hyderabad en 2008, à Sharm El Sheikh en 2009, à Vilnius en 2010, à Nairobi en 2011, à Bakou en 2012, à Bali en 2013 avec les mêmes objectifs, mettre en place une gouvernance partagée à l'échelle mondiale.

En analysant les conclusions de ces débats autour de la gouvernance d'Internet, nous avons constaté trois positions différentes :

- ***Une première position:***
  Portée par Les États-Unis, et soutenue par Israël, qui ne semble ne pas vouloir réduire son contrôle sur l'ensemble des instances gérants l'architecture d'Internet. En effet, Les États-Unis tiennent une légitimité de domination à partir des facteurs historiques et du fait qu'ils ont largement contribué au développement des infrastructures et à la mise en place d'une gouvernance de l'Internet telle qu'elle est aujourd'hui. Ainsi, cette position lui assure une avancée remarquable en termes de cyberespionnage, de cybersécurité et cybersurveillance comme en témoigne l'affaire PRISM par exemple. Ainsi, cette domination fait des États-Unis un Cyber-État très puissant ;

---

(1) Voir le site Internet dédié à l'événement : https://www.netmundial.org/fr/accueil

(2) D. FAYON, Géopolitique de l'Internet, Paris, Economica, 2013, P.1

- ***Une deuxième position*** :
  Portée par les BRICS, l'Iran, l'Arabie Saoudite et d'autres régimes semblables. Ces pays souhaitent placer ces instances de gouvernance sous le contrôle d'Union International des Télécommunications (IUT). En effet, ils désirent impliquer l'ensemble des États dans la définition des grandes orientations pour l'Internet de demain tout en respectant la cybersouveraineté de chaque Cyber-État. Ainsi, les instances actuelles ne seront plus sous influences américaine mais elles deviendront indépendantes mais soumises au contrôle des Cyber-États ;

- ***La troisième position :***
  Est celle des pays européens, dont la France, qui adoptent une position modérée, proche de celle des États-Unis. Ainsi, ils souhaitent empêcher que les différentes instances de régulation d'Internet ne soient soumises à des régimes « fermés ». Cependant, ils espèrent revoir les dispositifs actuels et réduire la domination américaine avec une implication plus significative de l'Union Européen.

Ainsi et depuis que l'économie mondiale s'est configurée autour des technologies numérique, du Cloud Computing et du Big data en particulier, l'Internet est devenu un espace de conflit cybergéopolitique susceptible de déclencher des cyberguerres et qui pourrait mettre fin à l'Internet tel qu'il est aujourd'hui. Ainsi, des tentatives de plier Internet, par des moyens techniques ou réglementaires, au respect des frontières nationales ainsi qu'à la construction des Internet régionaux. Ces tentatives n'ont pas abouties et Internet a pu garder son esprit universel et son caractère du bien commun à tous.

Pour qu'il reste un bien commun accessible et protéger l'Internet de tout conflit cybergéopolitique, une gouvernance élargie à l'échelle planétaire se positionne comme une alternative sérieuse pour assurer le bon fonctionnement du « réseau des réseaux ». Une telle gouvernance permettrait une gestion partagée des protocoles et des noms de domaines, ainsi que, des débats élargis sur l'évolution des réseaux, la neutralité du Net, le respect des cybersouverainetés, *etc*. Un constat confirmé par Milton Mueller qui souligne qu'une gouvernance élargie est « *l'ensemble des querelles et des délibérations sur la façon de gérer, coordonner, et façonner Internet pour refléter des politiques* »[(1)].

De son côté, Lawrence Solum[(2)] précise que la gouvernance d'Internet consisterait principalement en trois tâches principales :

[(1)] M. MUELLER, Networks and stats: The global politics of Internet governance, MIT Press, 2010, P.51.

[(2)] L. SOLUM, Models Of Internet governance, In Bygrave, L et Bing J 5Eds), Internet Governance: Infrastructure and Institution, 2009.

- Mettre au point les standards techniques et protocoles ;
- Allouer et assigner des ressources rares ;
- Formuler une politique, la mettre en œuvre et résoudre les éventuels conflits qu'elle engendre.

Une bonne gouvernance d'Internet prendrait également en compte à l'ensemble des questions essentielles ayant trait à la vie privée, à la liberté d'expression, à l'organisation des échanges, à la sécurité des personnes et des biens[(1)]. En effet, la protection des libertés fondamentales est devenue un sujet clé et fondamental au sein des différentes instances mondiale de gouvernance d'Internet où la position officielle de la France, pays des droits et des libertés, apparaît morcelée et peu audible. Cette position[(2)] est considérée déconnectée de celle des autres parties prenantes comme la société civile, le monde académique ou les entreprises privées, *etc*., et en particulier après les votes des lois antiterroristes et sur le renseignement.

Nous allons donc détaillé le fonctionnement de ces instances de contrôle d'Internet qualifiées par Pierre Monier comme une « république des ingénieurs »[(3)].

---

(1) G. DAN NGUYEN et S. DEJEAN, Le numérique : Economie de partage et de transactions, Economica, 2014.

(2) Cité dans rapport Ambition Numérique de Conseil National du Numérique, publié le 18 Juin 2015, p. 44.

(3) P. MOUNIER, Les maitres du réseau : les enjeux politiques d'Internet, La découverte, Paris, 2002.

B. « La république des ingénieurs » au service du Cyber-État

a) L'Internet Architecture Board (IAB)

L'Internet Architecture Board (IAB) (ou le conseil Architecture d'Internet) est une instance créée en 1984 et est chargée de coordonner l'orientation stratégique d'Internet opérée par IETF *(nous y reviendrons dans le prochain paragraphe)*. La RFC 2850[(1)] *(nous reviendrons dans cette partie sur la signification d'une RFC)* décrit le mode et la charte du fonctionnement de cette instance. Les RFC 3869[(2)] et RFC 1984[(3)] en précisent les missions confiées. Nous pouvons citer par exemple :

- Accompagner l'Internet Society (ISOC) [(4)] dans ses décisions ;
- Approuver les nominations proposées par le Comité de Nomination de l'IESG. L'Internet Engineering Steering Group (IESG) est un groupe de l'IETF chargé du pilotage de l'activité de production des standards Internet ;
- Approuver les nominations au sein de l'ICANN (nous la présenterons dans la suite de ce chapitre) ;
- Gérer et encadrer les relations de l'IETF avec les partenaires extérieurs.

L'Internet Architecture Board (IAB) est composée de 12 membres renouvelés tous les deux ans par moitié (soit 6 par an). Le président de l'IAB est nommé parmi ces 12 membres, ces derniers sont désignés par le « *Board of Trustees* » (ou conseil de confiance) de l'ISOC. Les membres de l'IAB portent une attention particulière aux activités émergentes de l'IETF, elle-même, issue de l'IAB comme nous allons le voir tout de suite.

---

(1) Voir http://tools.ietf.org/html/rfc2850

(2) Voir http://tools.ietf.org/html/rfc3869

(3) Voir http://tools.ietf.org/html/rfc1984

(4) L'ISOC apporte à l'Internet Engineering Task Force (IETF) un support organisationnel et financier. En retour, L'IETF doit nommer trois administrateurs de son bureau selon une procédure échelonnée sur trois ans et au rythme d'une nomination par an. Cette procédure est détaillée dans la « RFC 3677 - IETF ISOC Board of Trustee Appointment Procedures », adoptée en décembre 2003.

b) Internet Engineering Task Force (IETF)

Issue de l'IAB (Internet Achitecture Board), Internet Engineering Task Force IETF (ou « Détachement d'ingénierie d'Internet »). Elle se définit comme un groupe auto-organisé ou auto-institué qui contribue à la mise en œuvre des évolutions des technologies d'Internet. Elle a été créée par des bénévoles en 1986 et avait comme objectif de coordonner les processus d'élaboration des RFCs[(1)] pour l'évolution des protocoles de l'Internet. Cette institution contient 120 groupes de travail et organise trois rencontres annuelles pour valider l'ensemble des RFCs soumises par les contributeurs. Ces RFCs sont discutées en amont via des échanges électroniques par mails.

L'instance IETF trouve sa mission détaillé dans la RFC 13935[(2)]. En effet, les missions principales qui ressortent de cette RFC sont les suivantes:

- Spécifier le développement ou l'usage des protocoles Internet ;
- Identifier les techniques liées à l'Internet et proposer des solutions ;
- Favoriser l'échange d'informations entre tous les acteurs de l'Internet : fournisseurs de matériel, utilisateurs, chercheurs, opérateurs de réseaux et fournisseurs de services afin de garantir le bon fonctionnement et l'homogénéité de l'Internet.

Par la suite, la RFC 1391[(3)] définit les règles d'adhésion à ITEF. En effet, selon Mueller: « *il n'y'a pas d'adhésion à l'IETF. Tout le monde peut s'inscrire et participer à toutes les réunions. Ce qui caractérise l'appartenance à l'IETF c'est d'apparaitre sur une de ses listes de diffusion*»[(4)].

Le fonctionnement de base de l'ITEF se fait via des échanges électroniques. Cependant et vu l'augmentation de nombre des inscrits et l'accroissement des échanges par Internet, les rencontres physiques entre les membres ainsi qu'une organisation par groupe sont devenues la méthode officielle du travail afin de gérer les différentes demandes.

---

(1) Voir https://www.ietf.org/rfc/rfc3935

(2) Voir https://www.ietf.org/rfc/rfc1391

(3) Nous reviendrons sur le processus des RFC dans la suite de cette section

(4) M. MUELLER, Ruling the root: Internet governance and the taming of cyberspace, MIT Press, 2002, P.9.

Selon Lars Eggert[(1)], l'IETF organise trois rencontres annuelles avec la participation des personnes d'une cinquantaine de pays pour plus de 6500 RFCs publiées en 2012 dont une centaine publiées pour la France à travers Orange ou Alcatel Lucent. Du côté marocain, aucune RFC n'est déposée, ceci est dû principalement à l'absence des industriels marocains dans ce domaine. Cependant, nous remarquons une participation des universitaires marocains aux débats et aux discussions à l'image de Nabil Benamar, chercheur à l'université de Meknes au Maroc, qui était en charge de la première réunion 89 de l'IETF qui a eu lieu en mars 2014.

Pour gagner en efficacité, IETF est organisée en trois niveaux d'un point de vue hiérarchique. En effet, comme le montre Harald Alverstand[(2)], ITEF a trois niveaux principaux:

- *Niveau bas* : Les groupes de travail qui discutent les différentes RFCs soumises.
- *Niveau intermédiaire* : Les domaines. Cela concerne huit domaines au total : Applications (APP), General (GEN), Internet (INT), Operations and Management (OPS), Routing (RTG), Security (SEC), Transport (TSV), User Services (USV).
- *Niveau supérieur* : IESG (Internet Engineering Steering Group), groupe de pilotage chargé de mettre en œuvre les décisions de l'IETF. L'IESG évalue alors les propositions qui sont soumises sous la forme des RFCs temporaires.

Les adhérents de l'IETF pourront également être des employés des grandes entreprises privées. Ainsi, le risque avec une telle organisation c'est que ces membres, s'ils sont dans les instances décisionnelles, influencent les orientations et les choix de l'IETF en favorisant les intérêts de leurs employeurs. Cependant, il existe des mécanismes qui préviennent une telle dérive comme la concurrence entre les fournisseurs d'équipement : Cisco (américains), Alcatel (français), Huawei (chinois), *etc*. En effet, toutes ses entreprises se surveillent mutuellement dans les groupes du travail, mais également hors ce cadre comme en témoigne les affaires de cyberespionnage économique de la NSA, et les récentes lois françaises en la matière, dont celle de renseignement adoptée le 03 Octobre 2015, empêchant toute mauvaise orientation des décisions en fonctions d'intérêts liés à la sécurité nationale. Egalement, la présence des parties tierces indépendantes comme des chercheurs ont permis de maintenir l'esprit initial qui a fondé l'IETF[(3)]. Ainsi, cette cybersurveillance et ces rapports de force et de domination nous représentent les conflits d'intérêts dans un champ au sens de Bourdieu.

---

(1) L. EGGERT, From Research to Internet Standards, 30th Brazilian Symposium On Computer Networks and Distributed Systems. Ouro Preto, Bazil , 2012.

(2) H. ALVERSTAND, Development of Core Internet standards: The work of IETF and W3C, In Bygrave, L. et Bing J (Eds), p.126-149, 2009.

(3) H. ALVERSTAND, Development of Core Internet standards: The work of IETF and W3C, In Bygrave, L. et Bing J (Eds), p.126-149, 2009.

c) World Wide Web consortium (W3C)

A l'inverse des autres inventions liées à Internet d'origines américaines, le World Wide Web était quant à lui le produit de l'Organisation Européenne pour la Recherche Nucléaire (CERN) qui l'a mis à disposition de public à partir de 1989. Cependant, faute de l'absence d'une vision politique du long terme [(1)], son développement a été par la suite repris par les États-Unis faisant naissance en 1994 au World Wide Web Consortium (W3C) (ou Organisation pour le réseau mondial).

Ainsi, le W3C est un organisme de standardisation des technologies du Web comme les normes HTML, HTTP, XML, XHTML, CSS ou encore du format d'image PNG. Sa gestion est assurée conjointement par le MIT aux États-Unis, l'ERCIM[(2)] en Europe (dont l'INRIA français en fait partie), l'université Keio au Japon et l'université Beihang en Chine. Le W3C regroupent aujourd'hui 383 membres[(3)]. Parmi eux, on trouve les grandes entreprises comme IBM, Google, Facebook, Apple, Ali Baba Group,.., mais aussi des entreprises françaises comme Orange, SFR, Alcatel, *etc*.

Après sa mise à disposition par l'Organisation Européenne pour la Recherche Nucléaire (CERN), les États-Unis ont repris le développement de l'application World Wide Web et ont mis au point un navigateur Web, NSCA Mosaic, développé au National Center for Supercomputing Applications (NCSA), dans l'Illinois. Ce navigateur marque le début d'une guerre entre différents navigateurs avec la création d'Internet Explorer par Microsoft et Mozilla FireFox développé par la Fondation Mozilla avec l'aide de milliers de bénévoles.

Cette « guerre » — et tensions propres à ce champs —, concernant les navigateurs a vu la France, et l'Europe avec elle, s'éloigner et se marginalise définitivement alors qu'ils étaient à l'origine de l'invention. L'absence d'une vision politique visant à développer des solutions techniques pour Internet a fait de la France et de certains secteurs français, qu'ils soient publics ou privés, mais également des marocains, de simples utilisateurs d'Internet sans aucun pouvoir décisionnel dans les grandes orientations stratégiques. Pire encore, ce raté stratégique fait qu'aujourd'hui les pays européens, la France et l'Allemagne compris, subissent la cybersurveillance de la NSA et sont moins équipés pour une éventuelle cyberguerre.

---

(1) Rapport d'information du Sénat au nom de la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », par Mme Catherine MORIN-DESAILLY, 2013/2014, p.27

(2) L'ERCIM (acronyme signifiant en anglais European Research Consortium for Informatics and Mathematics) est une organisation ayant pour objectifs de stimuler la collaboration à l'intérieur de la communauté européenne de la recherche et d'augmenter la coopération avec l'industrie européenne. Voir le site officiel : http://www.ercim.eu/ , dernière consultation 08/07/2015 à 14h30.

(3) Voir la liste complète sur le site du W3C disponible http://www.w3.org/Consortium/Member/List, dernière consultation le 08/06/2015 à 15h.

Cette mise à l'écart de la France n'est que le résultat d'un manque d'une stratégie politique claire dans un domaine fondamental pour la sécurité et la souveraineté du pays. Un constat confirmé par Louis Pouzin[(1)] pendant son audition devant la commission sénatoriale chargée d'élaborer le rapport sur la gouvernance d'Internet :

> « *l'Europe est pratiquement restée muette depuis que l'on a abandonné l'idée d'être leader en matière de réseaux, dans les années 1970 et 1980. Faute de concurrence, ce sont essentiellement les Américains qui innovent dans ce domaine* […] *Nous n'en sommes que des utilisateurs, fort distants des lieux où s'élabore le futur*»[(2)].

La même constatation soulignée par David Fayon qui souligne qu'en France « *Nous manquons singulièrement d'ambition et de continuité dans l'action (…). Le général de Gaulle a lancé le Plan calcul, et depuis, il n'y a quasiment rien eu*» [(3)].

---

(1) Louis Pouzin est un des premiers ingénieurs français à s'intéresser à la discipline de l'informatique. Dans les années 1970, sur la base de ses connaissances acquises au MIT (Massachusetts Institute of Technology) et chez Bull, il dirige le projet Cyclades, un des premiers réseaux ordinateurs au sein de l'Iria (ex-Inria). Dans le cadre de ce projet, il créé le datagramme et le modèle de transmission des données par paquet. Ces travaux seront par la suite à l'origine de la création du protocole TCP/IP qui est la base d'Internet d'aujourd'hui.

(2) Rapport d'information du Sénat au nom de la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », par Mme Catherine MORIN-DESAILLY, 2013/2014, p.38.

(3) D.FAYON David dans Géopolitique de l'Internet, Paris, Economia, 2013, p. 48.

a) Internet Corporation for Assigned Names and Numbers (ICANN)

Comme nous le détaillons dans la prochaine partie dédiée à la gestion des protocoles, toutes les machines ont besoin d'un identifiant unique pour qu'elles puissent communiquer entre elles au sein d'un réseau informatique. Cet identifiant unique correspond à une adresse IP (Internet Protocole). Cette adresse est composée d'une série de chiffre seulement dans sa version 4 (IPv4) et des chiffres et des lettres dans sa version 6 (IPv6). Ainsi, pour identifier une machine sur un réseau informatique ou sur Internet, un utilisateur doit connaitre son adresse IP qui correspond à son identifiant unique.

Cependant, vu la multiplication des adresses (chaque site web et chaque machine ont une adresse IP dédiée), les architectes du réseau, et « les ingénieurs de la république », ont mis en place le Domain Name System (DNS) afin de simplifier la vie aux utilisateurs. En effet, ces utilisateurs retiennent seulement une chaine de caractère compréhensible du site web souhaité au lieu d'une série de chiffres. Par exemple: il est simple de retenir www.france.fr au lieu de 45.33.12.175[(1)]. L'objectif dans la mise en place d'un tel mécanisme n'était pas de contourner des contraintes techniques mais plutôt de permettre une navigation confortable aux utilisateurs[(2)].

Le Domain Name System (DNS) consiste donc à convertir un nom de domaine DNS vers une adresse numérique dans un réseau donné. La gestion des DNS est confiée à l'Internet Corporation for Assigned Names and Numbers (ICANN), dont l'organisation et les modes de fonctionnement suscitent des débats contre la domination des États-Unis.

ICANN ou Internet Corporation for Assigned Names and Numbers (la Société pour l'attribution des noms de domaine et des numéros sur Internet) est une entreprise fondée en 1998 de droit californien à but non lucratif. Dès sa création, l'ICANN a hérité de l'IANA (Internet Assigned Numbers Authority)[(3)] la gestion et l'assignation des adresses IP suite à un appel d'offre réalisé par le département du commerce américain. Le mode de fonctionnement de l'ICANN est décrit dans la RFC 920[(4)]. Bien qu'elle soit implantée en Californie, son autorité s'étend, directement ou indirectement, à tous les utilisateurs d'internet.

---

(1) Test réalisé le 08/07/2015. Le résultat est renvoyé via la commande informatique ping www.france.fr à partir d'une machine Windows.

(2) M. MUELLER, Ruling the root: Internet governance and the taming of cyberspace, MIT Press, 2002.

(3) IANA a été créée à l'initiative de Jon Postel éditeur des Requests for Comments (RFCs). Depuis 1998, elle est une composante de l'ICANN, l'autorité suprême de régulation de l'Internet.

(4) Voir https://www.ietf.org/rfc/rfc920

Ainsi, l'ICANN a le potentiel de changer radicalement la nature d'Internet en mettant en place tous les mécanismes nécessaires à la création, à la promulgation et au renforcement de la régulation. En effet, l'ICANN exerce une politique publique globale en s'appuyant sur les institutions de gouvernance (IAB, IETF, …) d'où elle tire sa légitimité.

Comme l'expliquent Dan Nguyen et Dejean[(3)], lorsqu'une organisation ou une entité souhaite mettre en place un site web et lui attribuer un patronyme, elle dépose un nom de domaine afin que l'ICANN lui attribue un DNS. Pour le faire, elle doit suivre ces étapes :

1) Elle doit d'abord choisir un TDL (Top Level Domain) dans lequel il souhaite le déposer. Concrètement, cela correspond au suffixe « .fr » ou « .com » ou autre parmi ceux qui sont disponibles. Ce suffixe correspond à une « zone ». L'espace des noms de domaines est donc partitionné ;

2) Par la suite, l'entité choisit de façon plus libre le nom de domaine de second niveau. Ce dernier correspond au nom véritable que l'entité souhaite donner à son site web. Par exemple : «*monproduit* » ;

3) Après un certain nombre de formalités, cette entité devient la propriétaire du nom de domaine « monproduit.fr » ou « monproduit.com » ;

4) Les clients de l'entité en question accéderont à son site web via leur navigateur en utilisant les adresses « www.monproduit.fr » ou « www.monproduit.com ».

---

(1) IANA a été créée à l'initiative de Jon Postel éditeur des Requests for Comments (RFCs). Depuis 1998, elle est une composante de l'ICANN, l'autorité suprême de régulation de l'Internet.

(2) Voir https://www.ietf.org/rfc/rfc920

(3) G. DAN NGUYEN et S. DEJEAN, Le numérique : Economie de partage et de transactions, Economica, 2014.

Dans les années 1980, la zone d'un nom de domaine était utilisée pour identifier le rattachement d'un utilisateur américain à une organisation spécifique. En effet, six noms de domaine du type gTLD (Global Top Level Domain) existent à l'époque. Il s'agit de:

- « *.gov* » destiné aux administrations fédérales américaines ;
- « *.edu* » destiné aux universités et instituts de formation américains ;
- « *.mil* » utilisé par e ministère de la défense américain ;
- « *.net* » utilisé par les fournisseurs d'infrastructures et de télécommunications ;
- « *.org* » utilisé par toutes autre institutions ;
- «*.com* » destiné aux entreprises et sera le plus demandé et utilisé.

Après l'internationalisation de l'Internet, des DNS sont inspirés du code postal de chaque pays comme « .fr » pour le France « .ma » pour le Maroc et « .de » pour l'Allemagne par exemple. Le schéma suivant montre la hiérarchie du nom de domaine pour Wikipédia:

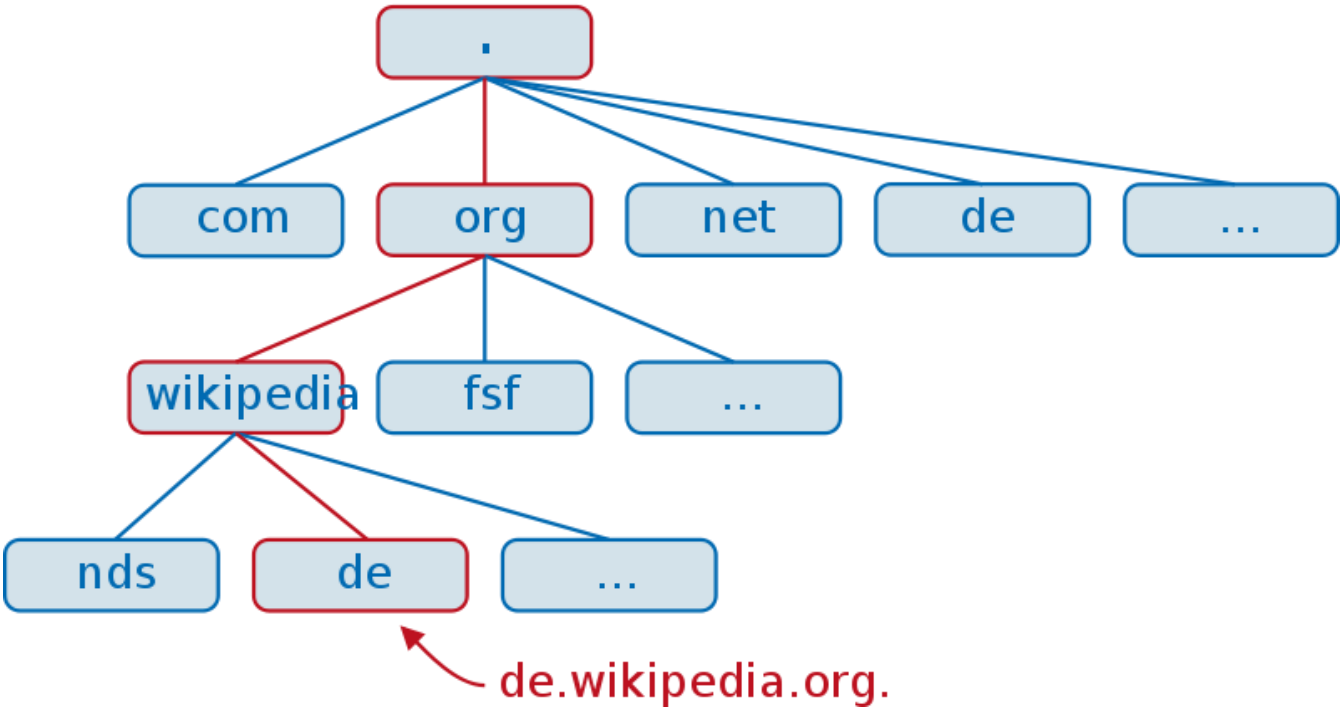


Figure 6 : Illustration la hiérarchie des noms de domaine pour Wikipédia[(1)]

---

(1) Image prise de Wikipédia à partir de http://commons.wikimedia.org/wiki/File:Dns-raum.svg

Comme le montre le schéma ci-dessus, au sommet de la pyramide existe un serveur racine qui prend la forme d'un point ***[.]***.

En effet, ce serveur est situé aux États-Unis et sous le contrôle de son département du commerce. Ce serveur contrôle la répartition des différents domaines en fonction de leurs zones géographiques («.fr », « .ma », « .uk », *etc*) ou par secteur d'activité («.com», «.net», «.org», *etc*). En plus, ce «serveur racine» contient un répertoire officiel qui permet de traduire les noms de domaines en adresse IP sachant que l'ICANN perçoit une « taxe » sur chaque nom de domaine attribué, en 2012, son montant s'élevait déjà à 90 millions d'euros de taxes perçues.

Ainsi, il est clair qu'avoir la main sur ce serveur central ayant toutes les adresses et les informations sur l'ensemble des sites web Internet mondiaux, permet à la NSA d'avoir un avantage sur les autres pays ainsi déployer ses programmes de cybersurveillance lui donnant un moyen efficace pour une éventuelle cyberguerre. A titre d'exemple, le mode de gestion des noms de domaines (www.monpays.com par exemple) permettrait d'isoler toute l'infrastructure Internet d'un pays donc isoler ce pays techniquement comme en témoigne l'arrêt d'Internet en Corée du Nord comme réponse américaine au piratage des données de l'entreprise Sony en 2014.

Le monopole du contrôle de la régulation d'Internet, les taxes perçues sur chaque transaction, et l'influence du gouvernement américain ont fait de l'ICANN la cible de nombreuses critiques venues de plusieurs pays comme en témoigne le conflit qui oppose la France à l' ICANN autour de l'extension « .vin » et qui montre le degrés de complexité de la gestion de l'infrastructure Internet. En effet, ICANN avait annonçait l'arrivée de milliers de nouveaux suffixes dont les « .vin » et « .wine ». Aucun des acteurs du secteur français des vins ou spiritueux n'est candidat à l'acquisition de ces domaines, autrement dit, les professionnels français n'ont pas eu le temps de se porter candidats pour acquérir ces nouveaux noms de domaine. Ils accusent le manque d'information et la grande opacité (voulue ?) de l'ICANN.

Apporter une réponse à ces questions de gouvernance est l'objectif de la mise en place du Forum sur la Gouvernance d'Internet (IGF) que nous avons vu au début de cette section. Ainsi, Bernard Benhamou[(1)] souligne que l'un des objectifs essentiels était d'inscrire la supervision de ces différentes infrastructures critiques dans un cadre qui soit à la fois multilatéral, transparent et démocratique.

---

(1) B. BENHAMOU, Organiser l'architecture de l'Internet, revue Esprit, Mai 2006.

C. Développement des protocoles et assignation d'adresses Internet (IP)

a) Le mécanisme d'élaboration des protocoles

Pour que deux ordinateurs puissent communiquer entre eux et que des services puissent être rendus aux utilisateurs, il faut définir des protocoles normalisés. Ces protocoles concernent des services et des usages spécifiques comme la vidéo, la téléphonie, *etc*. Le plus connu de ces protocoles et qui fait le noyau des échanges sur Internet est le protocole TCP/IP[(1)]. Ce protocole est largement utilisé grâce à sa robustesse et sa fiabilité. Une adresse IP (Internet Protocol) unique permet d'identifier un ordinateur sur un réseau donné. Par conséquent, les échanges entre plusieurs ordinateurs deviennent possibles grâce à cette adresse unique.

En effet, l'élaboration initiale des protocoles d'interfonctionnements des réseaux IP sur Arpanet[(2)] (d'origine militaire) puis sur Internet a été l'œuvre collective de la « République des ingénieurs ». L'objectif initial de ces ingénieurs, organisés d'une façon volontaire et informelle, était de développer un réseau d'échanges et non un réseau universel comme ce fut le cas pour le réseau téléphonique[(3)]. Les contributions volontaires et individuelles sont émises en toute indépendance institutionnelle. Ainsi, elles ont produit le système technique que l'on connait aujourd'hui considéré comme une « convention sociale » au sens des théories des conventions[(4)].

La procédure de création des protocoles suit un processus immuables depuis 1969. Cette procédure appelée « RFC » (Requests For Comments) est gérée par l'instance « IETF » (Internet Engineering Task Force) vu précédemment. Le principe de contribution est simple, chaque individu, volontaire ou non, peut proposer une évolution d'un protocole particulier. Par la suite, des différents groupes du travail se réunissent et produisent un document « RFC». Ce document suit un long processus de validation avant d'être validé et définitivement approuvé par l'instance suprême « IAB » (Internet Architecture Board).

---

(1) Le TCP/IP est l'ensemble des protocoles utilisés pour le transfert des données sur Internet. Il est souvent appelé TCP/IP : TCP (Transmission Control Protocol) et IP (Internet Protocol). Le document de référence est RFC 1122.

(2) Pour rappel, Arpanet (acronyme anglais de « Advanced Research Projects Agency Network », souvent typographié « ARPAnet »1) est le premier réseau à transfert de paquets développé aux États-Unis par la DARPA (Agence pour les projets de recherche avancée de défense). Le projet fut lancé en 1969 et la première démonstration officielle date d'octobre 1972.

(3) O. FAVEREAU, Règles, Organisation et Apprentissage collectif : Un paradigme non-standard pour trois théories hétérodoxes, 1992.

(4) La théorie de la convention est une théorie des institutions et des organisations qui explore la manière selon laquelle les individus décident dans des situations complexes et d'incertitude, décisions qui dépendent des ajustements de chacun, de la convergence et de l'auto-renforcement de l'harmonisation des comportements individuels. Il s'agit d'un courant de recherches qui s'est développé ces 20 dernières années se situant aux frontières de la sociologie, de l'économie et de la gestion. Source : http://www.wikiberal.org

Selon Laura De Nardis[(1)], les règles de gestion qui gèrent l'élaboration des « RFCs » et qui sont toujours en vigueur sont les suivantes :

- Les «RFCs» sont « éternelles » au sens où elles sont archivées et ne sont jamais effacées. L'objectif est de garder une trace même si une RFC n'est plus d'actualité. C'est-à-dire qu'une RFC plus récente remplace une RFC ancienne. La première RFC fut émise en 1969 et l'archive constitué depuis cette date par Jon Postel[(2)] constitue une mémoire collective d'Internet ;

- Les RFC sont discutées principalement par courrier électronique. L'inscription aux listes de diffusion est libre et sans restriction ;

- L'élaboration des «RFCs» suit un processus strict en plusieurs phases : Proposition de la RFC, discussion de la RFC, puis une version intermédiaire est approuvé par consensus, et une « RFC » devient un véritable standard après validation de « IAB » ;

- Les « RFCs » sont archivées une fois remplacées par des nouvelles « RFCs » qui les mettent à jour.

Ce mode de fonctionnement présente plusieurs avantages par son caractère flexible dû aux échanges via la voie électronique. Comme les propositions sont mises à disposition en libre accès sur Internet, elles sont rapidement discutées par toutes les personnes volontaires via des échanges mail. L'originalité de ce mode de fonctionnement réside dans son caractère universel et non contraignant pour approuver et valider des «RFCs». Cependant, on remarque la présence de mandataires des intérêts privés pour l'approbation et la promotion des nouveaux protocoles. En tête de ces intérêts privés, on trouve les constructeurs d'équipements réseaux. Comme l'illustre le graphe ci-dessous, le constructeur américain Cisco arrive en tête des contributeurs suivi par le chinois Huawei. Nous retrouvons également le même constat pour les universités, en effet, l'américaine MIT apparait en premier suivie par l'université chinoise Tsinghua.

---

(1) L. DE NARDIS, Protocol Politics: The Globalization Of Internet Gouvernance, MIT Press, P. 25-26-27, 2009.

(2) Jon Postel fut l'archiviste des RFCs , et selon De Nardis, il s'occupait également de l'administration et l'assignation des numéros des adresses IP.

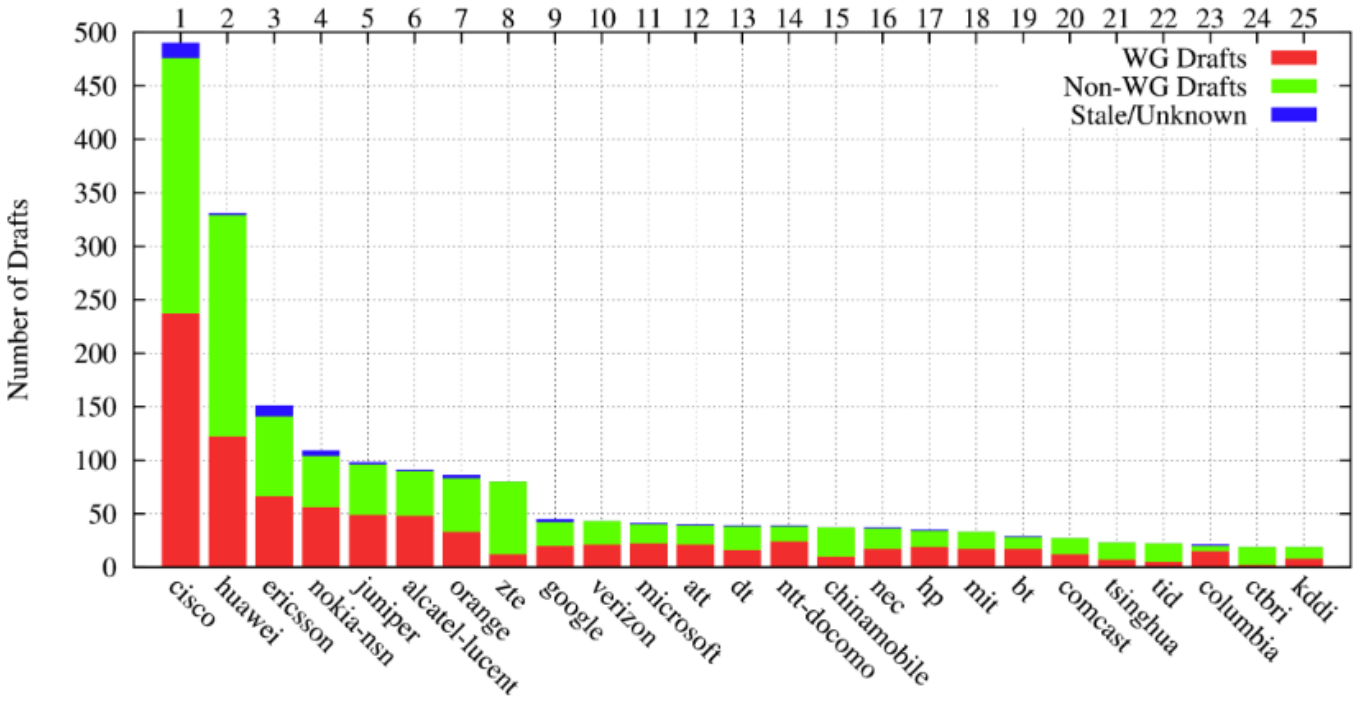


Figure 7 : Répartition des RFCs déposées par acteurs (Entreprises et universités)

En lisant le graphe précedant, nous remarquons une compétition entre les États-Unis, la Chine et l'Europe pour déposer le plus grand nombre de RFC afin de dominer ce secteur des protocoles Internet.

Ainsi, nous nous retrouvons encore une fois dans un champ au sens de Bourdieu dont les ressources principales sont les centres de recherches et développement publics et privés mais également les différents laboratoires de recherche des universités.

Comme pour tout autre standard, une fois une « RFC » est adoptée, nul n'est tenu de la respecter. Cependant, si un constructeur souhaite s'interconnecter aux autres équipements de d'autres constructeurs, il doit soumettre et respecter cette nouvelle RFC adoptée. Il s'agit finalement pour tous les constructeurs de s'inscrire dans une logique gagnant-gagnant.

Comme nous venons de le voir, le processus de contribution aux « RFCs » vient de mettre en place une innovation sociale et un savoir collectif fondé sur la base des contributions individuelles. Une organisation à laquelle se sont ralliées toutes les parties prenantes (entreprises privés, des volontaires, chercheurs, *etc*) mais qui subit de plus en plus des pressions des intérêts privés puissants et se trouve au centre des tensions entre les différentes entreprises et universités qui s'exprimes l'augmentation permanente des RFCs de changement des protocoles Internet émises par ces entreprises et universités.

b) Gestion des adresses Internet : Internet Protocol (IP)

Comme nous l'avons précisé au début de cette partie, pour que les ordinateurs puissent échanger des données sur Internet, ils doivent avoir un identifiant unique qui correspondant à une adresse IP (Internet Protocol).

Au début d'Internet et à l'époque du projet Arpanet, le problème de pénurie des adresses ne se posait pas vu que cela concernait que quelques milliers de machines interconnectées dans les universités américaines. A partir de 1983, la version 4 de l'IP (connue sous IPv4) fut adoptée. Les concepteurs de cette version ont vu large et ont anticipé l'évolution d'Internet qui atteindrait 4,3 milliards de machines. Actuellement, cette limité est déjà atteinte, et le nombre d'appareils connectés sur Internet est en constante augmentation tiré particulièrement par l'arrivée des « objets connectés ».

L'inquiétude par rapport à la pénurie des adresses IP a commencé au sein de l'IETF à partir des années 1990. Cette crainte était associée également aux méthodes de gestion et d'attribution de l'adressage IP qui favorisaient les organismes américains. Par ailleurs, jusqu'aux années 1990, l'assignation des adresses IP aux organisations suivait un processus simple. Il suffisait de faire une simple demande à Jon Postel qui était mandaté par « IAB » d'enregistrer les demandes. En 1990 et d'après Laura De Nardis[(1)]:

- 27% des blocs[(2)] de la classe A qui donnait droit à 16 millions d'adresses était déjà attribués principalement aux entreprises et aux universités américaines ;

- 15% du bloc de la classe B qui donnait accès à 65000 adresses ;

- Et seulement 1% du bloc de la classe C qui donnai accès à 256 adresses.

Par la suite, la pénurie de ces adresses commence à devenir un sérieux risque pour la stabilité d'Internet vu que les américains seuls ont pris la grande part des adresses laissant peu d'adresses disponibles aux autres. Ainsi, cela a poussé beaucoup de pays, particulièrement la Chine et la Russie, à développer leurs propres mécanismes réseaux et donc à avoir des Internet régionaux et à casser l'aspect universel d'Internet.

Pour y faire face et éviter le scénario d'avoir des réseaux Internet régionaux et non un seul Internet mondial, les deux mécanismes suivants ont été adoptés par IETF : CIDR (Class Less Interdomain Routing) permet de faire disparaitre la répartition par classe et NAT (Network Adresse Translation) permet pour un réseau privé d'avoir ses propres adresses et de se connecter au réseau public sans pour autant créer un Internet régional.

---

(1) L. DE NARDIS, Protocol Politics: The Globalization Of Internet Gouvernance, MIT Press, P. 25-26-27, 2009.

(2) Un numéro d'adresse IP était divisé en deux parties: l'adresse de son bloc (réseau) et son adresse dans ce bloc. Les routeurs réseaux n'avaient besoin que de stocker l'adresse du bloc.

Les deux mécanismes CIDR et NAT ont permis de retarder l'épuisement des adresses IPv4 jusqu'en 2011. Ainsi, la résolution définitive du problème devient inévitable.

Pour résoudre définitivement ce problème, l'« IAB » a adopté une version V6 du protocole IP. Cette version appelée IPv6 est l'aboutissement des travaux menés au sein de l'IETF au cours des années 1990 pour succéder à IPv4. Les spécifications de l'IPv6 ont été finalisées dans la RFC 24601[(3)] en décembre 1998. Le fonctionnement d'IPv6 est similaire à celui d'IPv4, les protocoles d'échanges sont pratiquement inchangés.

La nouvelle version IPv6 semble résoudre le problème de la pénurie des adresses IP. En effet, avec cette version, il y aura 340 millions de milliards de milliards de milliards d'adresses à attribuer, donc, inépuisables. Selon l'OCDE, la véritable difficulté consiste dans la transition de l'IPv4 vers l'IPv6. En effet, cette difficulté réside dans la compatibilité entre les deux versions. L'IPv6 n'est pas « rétro-compatible » avec l'IPv4. Plusieurs organisations sont donc sceptiques par rapport à cette migration et les constructeurs d'équipement ne maintiennent pas des systèmes de conversions entre les deux versions IPv6 et IPv4. A cela s'ajoute le fait que la prise de décision de migrer vers la nouvelle version est prise librement par l'organisation, ce qui implique des problèmes classique de coordination.

Au final, la pénurie des adresses IP dû au succès de l'Internet semble être résolue avec l'adoption de la nouvelle version IPv6 qui, certes, rencontre des difficultés d'adoption, mais, qui seront dépassées dans l'avenir. Cependant, la tutelle américaine sur l'assignation et le favoritisme affiché pour les organisations américaines a fini par poser des problèmes car de plus en plus d'ordinateurs connectés sur Internet sont situés hors le territoire des États-Unis. Cette tension a conduit à l'émergence des enregistreurs régionaux des adresses IPs mais, toutefois, reste sous le contrôle américain.

[(3)] Voir http://tools.ietf.org/html/rfc2460

D. Rapport de pouvoir dans la gouvernance d'Internet

L'Internet fait face aujourd'hui à une complexité de ses architectures mais également à sa gestion institutionnelle. En effet, comme le monde le schéma ci-dessous, plusieurs acteurs interviennent dans la définition des orientations stratégique de ces réseaux.

Tout d'abord, les institutions internationales que nous avons vues plus haut. Elles sont censées assurer une représentativité de tous les acteurs, assurer une bonne gouvernance et également sécuriser l'avenir et le développement du réseau Internet. Certaines institutions qui gèrent l'infrastructure techniques sont sous contrôle des Etats-Unis, et précisément les deux plus influentes ICANN et IETF. D'autres institutions parallèles sont plutôt gérées par l'Union International des Télécommunications (UIT) plus proche des régimes russes et chinois et qui contient également une représentativité des BRICS.

Le deuxième volet concerne les acteurs commerciaux ou les industriels de l'informatique et de l'électronique. En effet, comme le montre le schéma, une sélection d'acteurs influence le développement d'Internet selon leurs intérêts commerciaux mais également selon les orientations de leurs états d'appartenance. Par conséquent, les rapports de pouvoir entre États se déplacent au sein des entreprises du secteur majoritairement soutenu par des puissances publiques. Ainsi, les entreprises américaines dominent largement en termes de chiffre d'affaire réalisé, de brevets déposés mais également d'influence sur les choix stratégique d'Internet et le champ en question. Le tableau ci-dessous montre ainsi le classement de ces entreprises selon leurs chiffres d'affaire.

Ainsi, contrairement à son état d'esprit libertaire, Internet n'a jamais cessé d'être, conformément à ses origines historiques et technologiques, un outil aux mains de la puissance étatique en particulier l'administration américaine à travers sa main-mise sur la gestion de l'essentiel des infrastructures physiques qui en permettent le fonctionnement. Cependant, à l'instar du Brésil, beaucoup de pays manifestent leur mécontentement par rapport à cette domination américaine que ne fait que déplacer les enjeux géopolitiques vers le cyberspace dont les frontières ne sont pas reconnues car elles sont mouvantes et technologiquement en situation permanente de définition.

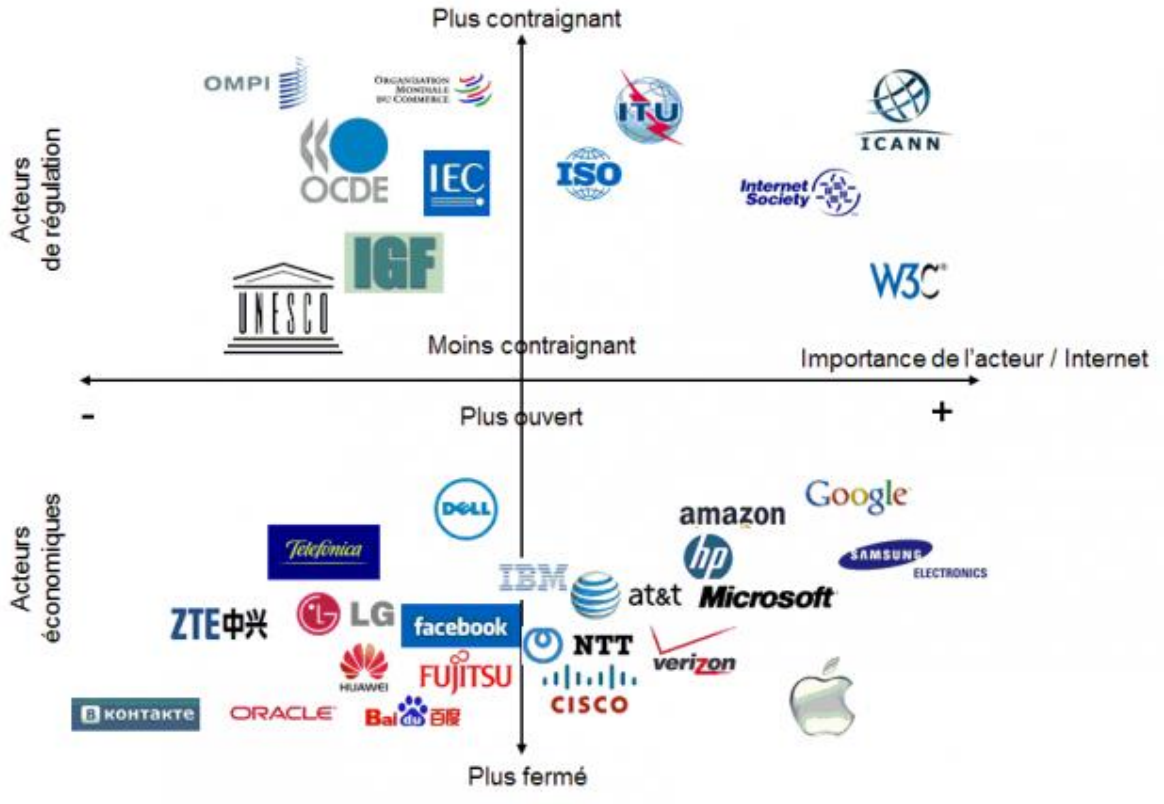


Figure 8 : Répartition des acteurs autour d'Internet (selon Fayon)

Rang	Pays	Nombre d'entreprises dans le Top 200	Chiffre d'affaires 2011 (en milliards de dollars)
1	États-Unis	38	1 219
2	Japon	23	937
3	Corée du Sud	8	253
4	Allemagne	4	202
5	Taïwan	9	198
6	Chine	6	177
7	France	7	166
8	Royaume-Uni	3	111
9	Espagne	2	84
10	Pays-Bas	3	55

Figure 9 : Classement des pays selon les entreprises numérique et leurs chiffres d'affaire (selon Fayon)

E. « Neutralité du Net » à l'ère du Cyber-État

a) Contexte :

Comme nous l'avons vu précédemment, l'internet est défini comme un réseau public mondial mais aussi comme un bien collectif commun à tous les cyber-citoyens. La transmission des données sont acheminées via un protocole TCP/IP (IPv4 et IPv6) dédié. L'accès à Internet aujourd'hui se fait via des réseaux fixes mais également à travers des réseaux mobiles : Wifi, 3G, 4G, *etc*. Ces derniers permettant de se connecter depuis des différents terminaux : ordinateurs, téléphones mobiles. Pour simplifier le schéma, il existe trois acteurs principaux qui interviennent dans le fonctionnement de l'Internet :

- *Les opérateurs télécoms* qui déploient et exploitent les réseaux et forment le maillage mondial ;
- *Les fournisseurs de contenus et d'applications (FCA),* qui proposent des plateformes de contenus et d'applications via des accès fixes ou mobiles. Ces plateformes sont principalement disponibles dans le Cloud ;
- *Les utilisateurs finaux* qui sont des personnes physiques ou morales qui accèdent au réseau pour leurs propres besoins, par l'intermédiaire de terminaux fixes ou mobiles.

b) Origines

L'article 11 de la Déclaration des Droits de l'Homme et du Citoyen énonce « *la libre communication des pensées et des opinions* ». En effet, Internet est un espace commun qui:

- Démocratise l'accès au savoir, comme le fut en son temps la révolution de l'imprimerie comme le souligne Michel Serres[(1)] ;
- Permet une participation des citoyens aux débats politiques ;
- Fait émergé facilement de nouvelles idées, de connaissance et de savoir ;
- Facilite la coopération entre acteurs de toutes tailles au sein d'une filière industrielle ;

Or aujourd'hui, l'accroissement du trafic, la multiplication des acteurs et des plateformes, ainsi que les pressions pour instaurer des mesures de blocage à l'ère de la cybersurveillance, les enjeux de cyberspace et de la cybersécurité, tous risquent de remettre en cause les règles fondamentales d'Internet. C'est ainsi qu'à partir de ce constat que l'on a vu naitre le débat autour de la « neutralité du Net ».

[(1)] M. SERRES, Petite Poucette , Paris, Editions le Pommier, 2012.

Ainsi, le traitement de ce sujet doit prendre en considération ces trois dimensions principales :

- *Dimension technique* :
  Le principe de neutralité de l'internet trouve son origine dans une question technique. En effet, Le réseau internet a été conçu pour fonctionner différemment des réseaux de téléphone classiques : il repose sur le principe du « routage de paquets » plutôt que de la « commutation de circuit ». De ce fait, le réseau internet est, historiquement, un réseau dont l'intelligence est située aux extrémités, dans les machines qui y sont connectées ;

- *Dimension économique :*
  Selon Nicholas Economides[(1)], la dimension économique réside dans les marchés dits bifaces, c'est-à-dire sur lesquels les intervenants peuvent se rémunérer sur deux catégories d'acteurs qu'ils mettent en relation, qui recommande qu'une des faces « subventionne » l'autre ;

- *Dimension juridique* :
  La dimension juridique révèle des questions liées à la liberté d'expression sur Internet, celle du blocage et du filtrage légaux et illégaux, surveillance en masse, cyber-droit, *etc*.

Le principe de la neutralité d'Internet fait débat grâce à des enjeux d'ordre technique, économique et éthique à savoir :

- L'accroissement, sur le marché fixe comme le mobile, du trafic Internet en générale et le trafic vidéo en particulier. Cela est dû principalement à la large diffusion des smartphones. Les coûts d'acheminement du trafic est couteux pour les fournisseurs d'accès Internet (FAI). Des investissements pour augmenter les capacités des réseaux existants et pouvoir absorber une quantité croissante de données sont nécessaires. D'autant plus que l'arrivée des phénomènes comme le Big data, l'«Internet des objets » et la diffusion des plateformes vidéo consommatrices en bande passante vont accentuer la problématique ;

---

(1) N. ECONOMIDES et J. TAG, Net Neutrality on the Internet: A Two-sided Market Analysis, New York University, 2007

(2) Rapport ARCEP au Parlement et au Gouvernement sur la neutralité de l'internet, 2012.

- La pression croissante des pouvoirs publics qui cherchent des moyens pour encadrer les activités sur Internet et faire respecter la loi. En effet, dans un rapport[(2)] de l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP), le débat sur la «neutralité de l'Internet » porte sur la question de savoir quel contrôle les acteurs de l'Internet ont le droit d'exercer sur le trafic acheminé, examiner les pratiques des opérateurs télécom sur leurs réseaux, et également leurs relations avec certains fournisseurs de contenus et d'applications ;

- La gestion de trafic à travers une différenciation des flux transitant sur les réseaux, par exemple en priorisant certains services ou en en ralentissant d'autres. Cette gestion est opérée à l'initiative des opérateurs par rapport à des probables contrats de partenariats publics ou privés. Par exemple, on peut imaginer un partenariat entre les deux entreprises comme Orange et la plateforme française de partage des vidéos Dailymotion. Le partenariat consisterait par exemple à prioriser les flux vidéos provenant de Dailymotion au sein des réseaux gérés par Orange qui est en relation étroite avec le dispositif de Défense de l'Etat français. Cette priorité donnée à Dailymotion impacterait la qualité du contenu rendu à l'utilisateur final par rapport à d'autres plateformes concurrentes comme Youtube ;

- Les fabricants de terminaux ou les fournisseurs de contenus et d'applications sont également concernés. Certains d'entre eux, particulièrement lorsqu'ils acquièrent une position importante sur leur marché, peuvent contribuer à favoriser certains contenus ou applications au détriment d'autres. Nous pouvons remarquer cela avec l'écosystème Appel qui contrôle strictement les applications destinées à ses propres terminaux.

Le débat comporte aussi une dimension sociétale et éthique en particulier sur le nécessaire équilibre à trouver entre la préservation des libertés fondamentales et individuelles, les obligations de la puissance publique légitimement imposer pour des raisons de sécurité nationale comme en témoigne par exemple les dispositifs de la loi relative au renseignement de 24 juillet 2015.

c) Eléments de définitions

Au sein de l'Instance IETF qui s'occupe de la gouvernance d'Internet, le terme «neutralité du Net » ne figure pas dans aucune des RFCs. En effet, selon Nicolas Curien et Winston Maxwell, ce terme a été utilisé par le professeur de Droit américain Tim Wu qui lui donne la définition suivante :

> «*Pour procurer une utilité maximale, un réseau public d'information doit tendre à un traitement équivalent de tous les contenus, sites et plateformes de façon à transporter tout type d'information et accepter toute application* »[(1)].

Ainsi, Curien et Maxwell clarifient la notion du « principe de neutralité » en soulignant que :

> « *Chaque utilisateur peut accéder librement à tous les contenus et tout contenu mis en ligne doit être accessible aux autres, sans restriction tarifaire ou technique* »[(2)].

A partir de ces deux conceptions, nous constatons que les fournisseurs d'accès à Internet doivent exclure toute forme de discrimination dans l'acheminement des flux Internet vers les utilisateurs. Pour Curien et Maxwell, les utilisateurs ont le droit d'accéder à tout contenu disponible en ligne selon le «principe de neutralité ». Il s'agit donc ici du principe d'égalité entre les cyber-citoyens face à un cyber-service publique dont le Cyber-État doit être le garant de son bon fonctionnement : neutralité des réseaux face aux services rendus.

Dans le cadre de la mise en place des règles communes pour le marché des télécommunications européen, le sujet autour de « la neutralité du Net » figure parmi les points abordés[(1)]. Ainsi, la neutralité y est définit comme :

[(1)] Curien Nicolas et Maxwell Winston, La neutralité d'Internet, La découverte, 2011, p. 10.

[(2)] Curien Nicolas et Maxwell Winston, La neutralité d'Internet, La découverte, 2011, p. 28.

« *Neutralité du réseau, le principe selon lequel l'ensemble du trafic Internet est traité de façon égale, sans discrimination, limitation ni interférence, indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application* […] *Les utilisateurs finaux sont en droit d'accéder aux informations et aux contenus et de les diffuser, d'exécuter et de fournir les applications et les services et d'utiliser les terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, ou quels que soient le lieu, l'origine ou la destination du service, de l'information ou du contenu, par l'intermédiaire de leur service d'accès à l'internet* […] *Les fournisseurs d'accès à l'internet, les fournisseurs de communications électroniques au public et les fournisseurs de contenus, d'applications et de services sont libres de proposer des services spécialisés aux utilisateurs finaux. Ces services ne sont proposés que si la capacité du réseau est suffisante pour les fournir en plus des services d'accès à l'internet et s'ils ne portent pas atteinte à la disponibilité ou à la qualité des services d'accès à l'internet. Les fournisseurs proposant un accès à l'internet aux utilisateurs finaux n'opèrent pas de discrimination entre des services ou des applications équivalents sur le plan fonctionnel* ». [(2)]

Ainsi, la « Neutralité du Net » renvoie vers le principe selon lequel l'ensemble du trafic de l'internet est traité de façon égale, sans discrimination et indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application utilisée. En particulier, la neutralité vise à garantir un traitement identique à tous les fournisseurs de contenus, petits ou grands, consensuels ou non. Symétriquement, les utilisateurs doivent pouvoir accéder aux informations et contenus de leurs choix sans discrimination. Cette définition a été reprise par le Federal Communications Commission (FCC)[(3)] dans son avis rendu en mars 2015 par rapport à ce principe de neutralité.

La « neutralité du Net » est un concept qui évolue avec l'avancée des techno-logies du numériques. En effet, malgré le fait qu'Internet et ses applications s'articulent autour des principes techniques simples (qu'il est important de protéger), la question de la « neutralité du Net » agrège des sujets qui viennent sans cesse s'ajouter les uns aux autres comme la cyberguerre, la cybersurveillance, le cyberespionnage, …, ou tout simplement la logique commerciale. En effet, le principe de neutralité des réseaux ne s'applique pas aux services dits «spécialisés » offerts par les opérateurs ne font pas partie de l'internet. La télévision ou la téléphonie, proposées dans les box Triple Play[(4)], sont autant de services spécialisés : ils sont délivrés sur des canaux dédiés, ne transitent pas par un réseau qui peut être temporairement surchargé ou inaccessible.

[(1)] Voir le communiqué de l'association Quadrature du Net à ce sujet. Disponible sur l'URL suivante : https://www.laquadrature.net/fr/neutralite-du-net-un-grand-pas-en-avant-pour-linternet-libre

[(2)] Voir l'Amendement 234 présenté par Marietje Schaake au nom du groupe ALDE et sous réf : A7-0190/2014.

[(3)] La Federal Communications Commission ou FCC est une agence du gouvernement des États-Unis créée par en 1934. Elle est chargée de réguler les télécommunications et Internet.

[(4)] Le triple play est une offre commerciale dans laquelle un opérateur propose à ses abonnés un ensemble de trois services dans le cadre d'un contrat unique : l'accès à l'Internet, la téléphonie et la télévision.

Afin de garder un espace libre loin de tout type de discrimination, l'association « La Quadrature du Net » a formulé plusieurs propositions[(2)] pour assurer par la loi une « neutralité du Net ». Nous citons par exemple :

- Inscrire dans la loi une définition d'Internet assise sur le principe de neutralité afin de garantir la pérennité de son architecture technique ;
- Le principe de neutralité doit s'appliquer à tous les réseaux Internet, quel que soit leur mode d'accès (fixe ou mobile). Les exceptions à ce principe, en cas de congestion non prévue ou de menace sur la sécurité du réseau, doivent être rigoureusement encadrées ;
- Les atteintes à la « neutralité du Net » par les opérateurs doivent faire l'objet de sanctions dissuasives ;
- Sur les réseaux, les conditions d'équilibre entre les « services gérés » et Internet sur les réseaux de communication doivent être pérennes afin de préserver la qualité de l'accès Internet ;
- Garantir la possibilité de s'exprimer anonymement en ligne.

Comme nous venons de le voir, la mobilisation autour du principe de la « neutralité du Net » est faite autour des principes suivants :

- La volonté de maintenir en l'État l'architecture de l'Internet loin de tout pouvoir d'influence politique ou économique ;
- Préserver la liberté donnée aux utilisateurs pour innover et développer des nouveaux services ;
- Préserver un espace où se pratique librement la liberté d'expression.

Ainsi, Hervé Crosnier[(2)] souligne que le débat autour de ce sujet déborde largement de son cadre technique et devient une oriflamme politique et un enjeu de géopolitique. En effet, il traduit un rapport de force entre Cyber-État, ainsi, chaque Cyber-État tente de favoriser ses propres flux et celui de ses entreprises ainsi bloquer ceux des autres. D'un autre côté, un Cyber-État peut favoriser l'accès des cyber-citoyens à un contenu particulier, qui serve ses propres intérêts de sécurité ou autre, au détriment de d'autres services plutôt à l'inverse de son orientation politique. Ainsi, le non-respect des principes de Neutralité risque de mettre le cyberspace sous une cybersurveillance ou tout le monde surveille le trafic de tout le monde … ainsi voir d'autres affaires Snowden surgissent.

[(1)] Voir l'ensemble des propositions sur http://www.laquadrature.net/files/Propositions_FR.pdf, dernière consultation 06/07/2015 à 18h45.

[(2)] H. CROSNIER , V. SCHAEFER et F. MUSIANI, La neutralité de l'Internet : enjeux de communication, CNRS édition, 2011.

F. Les aspects géopolitiques de l'affaire Snowden

a) Rappel du contexte

L'affaire Snowden a permis de rendre publiquement par l'intermédiaire des médias, notamment Le Guardian[(1)] et le Washington Post[(2)], des informations classées top-secrètes de la NSA[(3)] concernant des programmes de surveillance de masse comme PRISM[(4)] et autres. En effet, ces révélations ont montré que les collectes massives d'informations par la NSA, concernant des citoyens du monde entier, dépassent le cadre de la lutte nécessaire contre le terrorisme ou contre les autres risques géopolitiques mais ils s'inscrivent dans une continuité des programmes de surveillance depuis la deuxième guerre mondiale. Snowden justifie ses actions en indiquant que son « *seul objectif est de dire au public ce qui est fait en son nom et ce qui est fait contre lui* »[(5)].

Pour reprendre chronologiquement les événements :

- Le 5 Juin 2013 : Le Washington Post et le Guardian ont publié une note secrète sous le code s.125 de Patriot Act incitant l'opérateur Télécom Verizon à fournir à la NSA les détails des appels téléphoniques de tous les citoyens américains ;
- Le 6 Juin 2013 : Les deux journaux ont révélé l'existence d'un vaste programme de surveillance de la NSA nommé PRISM permettant l'accès aux données hébergées par les grandes entreprises du web américains. Ces mêmes entreprises sont également les principaux fournisseurs des solutions Cloud Computing. Dans la même journée, le directeur de la NSA, ADAM Clapper, a reconnu officiellement l'existence de ce programme en précisant qu'il est lié au FISA Amendment 2008 s.1881a/702 ;
- Le 7 Juin : L'identité d'Edward Snowde est révélée publiquement par le Washington Post et le Guardian ;
- Le 09 Juin 2013 : Edward Snowden, ex consultant de la NSA, a volontairement révélé les différents détails de ce programme d'espionnage dans une interview à un journal chinois.

---

(1) Glenn Greenwald, Ewen MacAskill et Laura Poitras, « Edward Snowden: the whistleblower behind the NSA surveillance revelations », The Guardian, 10 juin 2013.

(2) Barton Gellman, Aaron Blake et Greg Miller, « Edward Snowden comes forward as source of NSA leaks»,The Washington Post, 9 juin 2013.

(3) La National Security Agency (NSA, « Agence nationale de la sécurité ») est un organisme gouvernemental du département de la Défense des États-Unis, responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information et de traitement des données du gouvernement américain.

(4) PRISM, également appelé US-984XN1, est un programme de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques. Ce programme relevant de la National Security Agency (NSA) prévoit le ciblage de personnes vivant hors des États-Unis10. PRISM est supervisé par la United States Foreign Intelligence Surveillance Court (FISC) conformément au FISA Amendments Act of 2008 (FISA).

(5) Tanguy Berthemet, « Edward Snowden, l'homme qui fait trembler le gouvernement américain », Le Figaro.fr - 10 juin 2013.

Ainsi, l'affaire Snowden n'est pas une simple affaire de renseignement ou une affaire seulement politique, elle a eu des conséquences géopolitiques et précisément au niveau du cyberspace. Ainsi, cette affaire a remis en cause toute la gouvernance actuelle d'Internet et ses institutions, le développement des fondements techniques d'internet mais également le principe de neutralité de ses réseaux.

b) L'ennemi n'est plus seulement la Chine

Avant la révélation des affaires Snowden et Wikileaks, nous avons constaté une dénonciation accrue d'une menace de cyberespionnage massive des pays européens et des États-Unis par la Chine. En effet, un rapport sénatorial[(1)] pointe du doigt les liens entre les industriels chinois ZTE et Huawei (dont l'État Chinois est actionnaire) et le pouvoir central communiste chinois. Ce rapport liste dix priorités stratégiques pour la France et préconise quarante recommandations. L'une des priorités listées par ce rapport, la dixième, propose :

> « […] *d'interdire sur le territoire national et à l'échelle européenne le déploiement et l'utilisation de routeurs ou d'autres équipements de cœur de réseaux qui présentent un risque pour la sécurité nationale, en particulier les routeurs et certains équipements d'origine chinoise*».

Dans le même contexte, une situation similaire est constatée aux États-Unis. En effet, un rapport du Congrès préconise également le bannissement des équipements télécoms chinois appartenant aux mêmes entreprises Huawei et ZTE.

Cependant, comme le souligne Pierre Conesa[(2)], l'affaire Snowden a mis terme à une « fabrication de l'ennemi » par les États-Unis alors que ce pays est le champion d'espionnage cybernétique. Ainsi, Olivier Kempf se demande : « *Comment dénoncer l'espionnage chinois si on est soi-même le plus grand espion du monde ?* ».[(3)]

---

(1) Le rapport d'information sénatorial n° 681 (2011-2012) de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012.

(2) P. CONESA, La fabrication de l'ennemi ou comment tuer avec la conscience pour soi, Robert Laffont, 2011.

(3) O. KEMPF, L'affaire Snowden: Une rupture stratégique, Economica, 2015, P.138.

c) Vers une balkanisaton du Cyberspace

L'affaire Snowden a favorisé une balkanisation de cyberspace ainsi que les mesures nationalistes de protection (ou le cyber-nationalisme).

La balkanisation dans son sens propre désigne le phénomène des guerres balkaniques au début de XXème siècle. Par la suite, ce terme a pris une acceptation métaphorique et désigne la fragmentation souveraine d'espace préalablement intégrés. Ainsi, cette définition du terme nous renvoie vers cette fragmentation au niveau de cyberspace suite à l'affaire Snwoden. En effet, la balkanisation de cyberspace n'est pas d'ordre technique mais d'ordre politique provoqué principalement par cette de cyberespionnage américain. Ainsi, en remettant en cause la notion des souverainetés politiques des États et la cybersouveraineté des Cyber-États, révèle qu'il ne s'agit pas que de la Russie et la Chine qui peuvent conduire des opérations d'écoutes et d'espionnages massives, comme il le laisse entendre le processus de fabrication de l'ennemi par les États-Unis, mais tous les pays sont susceptibles de faire pareil malgré l'ensemble des accords de coopération les plus fiables. Par conséquent, les rapports de confiance entre les différentes Cyber-États, des nations historiquement liées entre-elles, se sont affaiblis confirmant ainsi que dans un cybergéopolitique, l'ami n'existe pas.

Cette affaire a rendu la balkanisation de cyberspace plus visible en lui donnant un coup d'accélérateur et en renforçant le cyber-nationalisme. Par conséquent, une course vers une autonomie technologique au niveau de cyberspace s'est déclenchée rendant de plus en plus les systèmes techniques fermés et verrouillés. Ce verrouillage rend le cyberspace déstructuré où l'intérêt souverain prime sur le reste. Ainsi, c'est toute la gouvernance qui se voit finalement heurter aux limites imposées par le pouvoir des Cyber-États.

Partie 3

Fondements techniques du Cyber-État

III. Partie 3 : Fondements techniques du Cyber-État

L'objectif de cette section est de comprendre, techniquement et fonctionnellement, l'ensemble des technologies étudiées. Ainsi, il s'agit de comprendre le fonctionnement de l'Internet, de Cloud Computing. Nous essayerons d'expliquer le lien entre ces différentes technologies ainsi que les différentes évolutions possibles.

Cette section se décompose en deux axes principaux :

- Le premier axe est dédié à une présentation de l'Internet et son rôle dans la transformation numérique en cours. Nous y présenterons également l'apport de l'Internet dans le développement des technologies étudiées : Le Cloud Computing et le Big data. Les thèmes de cette partie sont donc :
    - Le développement de l'Internet ;
    - Le rôle de l'Internet dans le fonctionnement du Cyber-État.

- Le second axe traite du Cloud Computing. Dans cette partie nous présenterons une revue de littérature de Cloud Computing et ses différentes définitions et ses architectures et ses modèles de déploiement. Nous essayerons de clarifier les différentes notions liées au Cloud Computing et nous finirons par une présentation des plans Cloud français et marocain ainsi que la notion du Cloud souverain. Dans cette partie, nous traiterons donc :

    - Le Cloud comme fondement technique du Cyber-État ;
    - Le Cloud souverain à l'ère de Cyber-État ;
    - Vers des référentiels de confiance à l'ère de Cloud ;
    - Quel Cloud pour le Cyber-État marocain ;
    - Le plan Cloud dans le cadre de a nouvelle France industrielle.

1. Chapitre 1 : Fondements techniques du Cyber-État : Internet

A. Développement de l'Internet

Selon Gilles Barouch et Hervé Chavas[(1)], un système technique numérique se caractérise par l'articulation de trois éléments principaux:

- Les composants électroniques qui grâce à la loi « de Moore »[(2)] poussent le progrès technique dans les deux autres éléments qui suivent ;
- Les terminaux qui traitent l'information et permettent d'en afficher le contenu ;
- Le réseau qui relie ces terminaux et qui permet à l'information d'être transmise.

Dans le contexte de notre recherche, nous attribuons le terme du système technique aux technologies suivantes : *Cloud Computing* qui permet de stocker les informations et héberger à distance des applications informatique, entre autres, de type *Big data*;

Ainsi, Barouch et Chavas considèrent que tout système technique est un vecteur d'innovation tant économique que social. Nous estimons que le système technique dans le cadre de notre recherche est également un vecteur de modification et transformation de l'économique et du social à travers l'ensemble des transformations qu'il opère dans plusieurs secteurs d'activités : Secteur de transport avec la plateforme *Uber*, secteur de l'immobilier avec la plateforme *AirBnB*, le secteur des voyages avec Booking.com, *etc*.

Ainsi, dans un système technique à base de Cloud Computing et de Big data, l'Internet y occupe une place originale et essentielle. Cependant, l'évolution de l'Internet n'est pas seulement liée aux facteurs techniques mais aussi à d'autres facteurs d'ordre politique, économique et social. Tous ont participé à l'émergence de l'Internet tel qu'il est aujourd'hui.

En effet, Internet est un groupe des réseaux interconnectés, eux-mêmes assemblages de plusieurs composants : appareils de transmission, des routeurs, des passerelles, des boxes, des logiciels, des serveurs et des ordinateurs dotés des processeurs. Aujourd'hui, ces processeurs sont également incorporés dans d'autres appareils comme les téléphones, les voitures, les réfrigérateurs, …, tous ces appareils sont capables de se connecter à Internet et interpréter ses différentes instructions. Internet assure donc le fonctionnement et l'interfonctionnement de tous ces objets communicants et s'insère de plus en plus dans nos vies quotidiennes.

---

(1) G. BAROUCH, H. CHAVAS, Où va la modernisation ? Dix années de modernisation de l'administration d'état en France, Harmattan, 1993.

(2) Cofondateur de la société Intel, Gordon Moore avait affirmé dès 1965 que le nombre de transistors par circuit de même taille allait doubler, à prix constants, tous les ans. Il rectifia par la suite en portant à dix-huit mois le rythme de doublement. Il en déduisit que la puissance des ordinateurs allait croître de manière exponentielle, et ce pour des années. Il avait raison. Sa loi, fondée sur un constat empirique, a été vérifiée

jusqu'à aujourd'hui. Il a cependant déclaré en 1997 que cette croissance des performances des puces se heurterait aux environs de 2017 à une limite physique : celle de la taille des atomes.

D'un point de vue purement technique, Internet fut une révolution par son caractère révolutionnaire des réseaux par rapport à ceux de la téléphonie mis en place à l'époque. Comme nous l'avons vu, Internet est né en 1969 d'un projet d'une agence fédérale américaine : la DARPA[(1)] qui dépendait du Pentagone américain. Ce projet ai fait naissance à un réseau qui s'appelait ARPANET[(2)] et qui porterai en 1983 le nom d'Internet au moment où le réseau militaire, utilisé par l'armée américaine, et le réseau civile, utilisé par le grand public, se séparent.

Ainsi, le terme Internet est d'origine américaine et est dérivé du concept d'internetting (en français : « interconnecter des réseaux ») dont la première utilisation documentée remonte à octobre 1972 par Robert Elliot Kahn[(3)] au cours de la première International Conference on Computer Communications (ICCC) [(4)] à Washington.

L'objectif de départ du projet Arpanet était de mettre en place un réseau différent de celui de la téléphonie et qui permet de relier l'ensemble des universités américaines qui étaient en contrat avec l'agence DARPA. Ainsi, cela a permis de partager la puissance de calcul des machines que possèdent les ordinateurs de chaque université. L'objectif recherché était donc de connecter l'ensemble de ces ordinateurs universitaires et de consolider leur puissance technique.

Pour se différencier des réseaux téléphoniques, les concepteurs d'Internet ont proposé une architecture complétement différente dont les principes se résument aux points suivants :

- Une transmission des messages par paquet et non plus par circuit comme ce fut le cas dans le réseau téléphonique ;

- L'architecture en couche permet l'indépendance de la communication vis-à-vis du matériel connecté ;

---

(1) La Defense Advanced Research Projects Agency (DARPA, « Agence pour les projets de recherche avancée de défense ») est une agence du département de la Défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire.

(2) ARPANET ou Arpanet (acronyme anglais de « Advanced Research Projects Agency Network », souvent typographié « ARPAnet ») est le premier réseau à transfert de paquets développé aux États-Unis par la DARPA. Le projet fut lancé en 1969 et la première démonstration officielle date d'octobre 1972.

(3) Robert Elliot Kahn, dit Bob Kahn (né le 23 décembre 1938, Brooklyn, New York) est un ingénieur américain au DARPA et co-inventeur avec Vinton Cerf du protocole TCP/IP. Nous y reviendrons dans la section 6.

(4) International Conference on Computer Communications est la première conférence publique pour présenter les technologies d'Internet et ses fonctionnalités comme produits du projet Arpanet. Elle a eu lieu entre 24 et 26 Octobre 1972 à Washington aux États-Unis.

- Mise en place de routage au lieu de commutation dans le réseau téléphonique. Ce routage permet aux extrémités (les apparies connectées) de contrôler le flux de l'information envoyée ;

- Des protocoles ouverts pour faire communiquer les flux différents couches et interconnecter les différents réseaux gérés par différents opérateurs ;

- Chaque réseau Internet fait de son mieux pour acheminer un flux et aucun flux n'est prioriser par rapport à d'autres. Ce principe est actuellement remis en cause avec tous les débats autour de la neutralité du Net ;

- Aucune tarification d'interconnexion entre les différents réseaux de différents opérateurs si ils sont de taille comparable.

Tous ces principes sont le fruit des années du travail et de négociation entre 1969 et 1983, la date de mise en place des spécificités de TCP/IP (nous y reviendrons dans la section 6).

L'internet ayant été popularisé par l'apparition du World Wide Web (nous y reviendrons dans la section 6), les deux sont parfois confondus par le public non averti. Ainsi, l'accès à l'Internet peut être obtenu grâce à un fournisseur d'accès à Internet via divers moyens de communication électronique : soit filaire (réseau téléphonique commuté (bas débit), ADSL, fibre optique), soit sans fil (WiMAX, par satellite, 3G+, 4G, *etc.*).

B. Le rôle de l'Internet au quotidien

Dans un Cyber-État, l'Internet est devenu indispensable et vitale au même titre que l'eau et l'électricité pour un État. En effet, son accès est nécessaire pour l'exercice d'activités et de droits fondamentaux par les citoyens : Réservation des voyages, démarches administratives, *etc*. Cependant, la complexité de ses architectures techniques et la criticité de ses réseaux supposent une gestion impartiale entre les différents États afin d'assurer son développement dans l'avenir et préserver son caractère comme bien commun à tous.

Ainsi, l'organisation des réseaux des télécommunications aujourd'hui montre une marginalisation des opérateurs télécoms censés assurer l'avenir de l'architecture technique d'Internet. En effet, leurs recettes sont en constante diminution depuis l'arrivée des plateformes de contenu Cloud Computing comme Youtube, Netflex, Facebook, *etc*. Pour y faire face, les opérateurs tentent de récompenser le manque à gagner via leur métier e Fournisseur d' Accès à Internet (FAI) ou à travers des aides publiques qui permettent de maintenir le bon fonctionnement des réseaux mais également du Cyber-État.

Selon l'OCDE[(1)], les réseaux Internet gérés par les opérateurs servent comme un canal aux plateformes de distribution de contenus qui de plus en plus dominent le cyberspace et multiplient les services et produits proposés aux utilisateurs. Cette évolution va à l'encontre de la conception initiale de l'architecture d'Internet qui n'a pas prévu une telle évolution mais plutôt un réseau ayant comme fonction principale l'acheminement des flux et des données entre universités.

D'un autre côté, le principe de domination des plateformes de contenus renforcent les craintes des utilisateurs par rapport à leurs données collectées en contrepartie des services proposés plus au moins gratuitement. Ces données sont commercialisées puis monétisées par les plateformes en question. Ainsi, le Cyber-État se trouvent face à des nouvelles contraintes techniques et juridiques afin de garantir un accès sécurisé et équitable pour tous ses citoyens. En effet, l'accès à Internet et aux réseaux est une mission de « cyber-service public » donc qui relève des missions du Cyber-État. Le principe d'égalité consiste à couvrir tous les territoires et tous les citoyens avec la même qualité et sans discrimination. Cette mission est loin d'être respectée pour des raisons techniques mais principalement commerciales.

Cependant, l'arrivée des plateformes du contenu vidéo de type Youtube et Netflex, etc., la bande passante réseau utilisée (canal de transmission des données) se voit de plus en plus dégradée par la consumation accrue de ces contenus par les utilisateurs. Ainsi, Le Cyber-État se dirige, par conséquent, vers des nouveaux modèles de taxation pour ces plateformes Internet. L'objectif recherché est de compenser financièrement les investissements dédiés à maintenir les installations existantes, rembourser les fonds publics investis, améliorer la qualité de la connectivité ainsi qu'absorber la demande croissante de la vidéo. Cependant, cette taxation fait débat et fait face à des systèmes de fiscalité très variés selon chaque pays. Par conséquent, le Cyber-État doit coopérer avec les autres Cyber-État pour mettre en place une politique fiscale commune ou dans le cas inverse, une solution radicale qui consiste à bloquer, à partir d'un certain seuil, la bande passante de chaque plateforme.

---

(1) Rapport OCDE Exploring the Economics of the Personal Data OECD Digital Economic paper, n° 200 OECD Publishing, 2013.

2. Chapitre 2. Fondements techniques du Cyber-État : le *Cloud Computing*

A. Introduction

a) Contexte

Le Cloud Computing peut être considéré comme un vecteur de démocratisation d'accès aux ressources informatiques pour les entreprises mais également pour les particuliers. En effet, il permet les utilisateurs peuvent utiliser des ressources informatiques indépendamment de leurs localisation géographique et des contraintes temporelles. Il leur suffit d'avoir une connexion Internet et un terminal électronique adapté. Ainsi, l'absence des barrières géographiques et temporelle n'est qu'une caractéristique du Cyber-État pour qui les frontières terrestres n'existent pas.

Ainsi, la technologie du Cloud Computing se résume principalement aux points suivants :

- Une consommation des services à travers Internet, telle que la messagerie électronique comme la solution Gmail.com de l'américain Google, Hotmail.com de l'américain Microsoft, Yahoo mail de 'américain Yahoo!, *etc.* ;

- Une gestion abstraite du logiciel informatique d'un point de vue utilisateur. Cette gestion concerne le software (programmes, ERP, antivirus, outils de gestion, etc) et le matériel informatique (machines, câbles réseaux, etc.). Ainsi, les utilisateurs se concentrent sur leurs activités principales : la vente, les achats, la construction, *etc*.

- Un libre accès aux ressources informatiques, via Internet ou à travers un réseau dédié, depuis n'importe quel endroit et à tout moment avec un paiement flexible selon la consommation et selon des règles tarifaires avantageuses pour les clients ;

- Un accès via une interface web depuis PC, tablette ou smartphone. Cet accès permet d'augmenter ou réduire les ressources allouer, générer des reporting sur l'utilisation de son informatique. Bref, une gestion complète à travers une interface web dédiées.

Par conséquent, le cloud Computing offre un moyen flexible et facile pour adopter des technologies numérique. Ainsi, il permet également le développement du « cyber-service public » à travers des cyber-politiques publiques et par la suite le développement du Cyber-État.

b) Emergence du Cloud Computing

Le concept de Cloud Computing n'est pas vu de la même façon selon les différentes perceptions de chaque individu. En effet, certains, que nous appelons des « *Cloudphobes*»[(1)], y voient un buzz marketing et un nouveau terrain de jeu propulsé par les grandes entreprises. D'autres, au contraire, y voient un nouveau paradigme qui va changer la façon dont l'informatique est traitée et utilisée au sein des organisations. Nous qualifions ces derniers des « *Cloudphiles*»[(2)].

En effet, La technologies du Cloud Computing n'est pas nouvelle en elle-même. Son apparition remonte aux débuts de l'informatique dans les années 1970. Ainsi, le Cloud Computing est considéré comme la suite logique de l'évolution des systèmes informatiques dès la naissance des «*mainframes* » (les grands ordinateurs centraux avec une grande puissance de calcul) en passant par l'architecture informatique Client-Serveur[(3)] dans les années 1980 puis l'architecture TCP/IP[(5)] durant les années 1990 qui a largement profité au développement du Cloud Computing. Au début des années 2000, c'est le tour de l'architecture SOA[(5)] de pousser le développement du Cloud Computing vers une utilisation massive.

Ainsi, le Cloud Computing s'est inscrit dans une continuité naturelle du développement des architectures informatiques et a été poussé, d'une part, par l'évolution des usages (Diffusion des plateformes Internet, Messagerie électronique, *etc*.), et d'autre part, par les contraintes technologiques et économiques des organisations : logique de réduction des coûts informatiques, concentration sur le cœur du métier, *etc*.

---

(1) et (2) A travers nos différents recherches autour des technologies Cloud Computing, nous nous sommes rendus compte que deux perceptions opposées existent d'où notre choix pour les deux termes « Cloudphobe » et « Cloudphile » pour qualifier les deux tendances. Nous, en tant que chercheur, nous nous positionnons comme «Cloudphile». Nous sommes persuadé que le Cloud Computing est une opportunité du développement technique mais également social à travers l'ensemble des activités numériques supportées : Accès à l'information, télémédecine, services à distance, développement du Cyber-État, etc.

(3) L'architecture client-serveur désigne un mode de communication à travers un réseau entre deux ou plusieurs machines : l'une, qualifiée de client, envoie des requêtes (demandes) ; l'autre ou les autres, qualifiées de serveurs, attendent les requêtes (demandent) des clients et y répondent.

(4) Le concept de l'architecture TCP/IP est développé dans la section 6.

(5) L'architecture orientée services (de l'anglais Service Oriented Architecture, SOA) est une forme d'architecture de médiation qui est un modèle d'interaction qui met en œuvre les échanges entre les services Internet. Ce terme est apparu au début des années 2000s pour pallier aux problématiques d'interopérabilité entre différents services informatiques exposés sur Internet.

Cependant, le développement de Cloud Computing a pu bénitier des projets de Recherche et Développement (R&D) menés principalement par des entreprises traditionnelles et historiques dans l'industrie informatique comme IBM, HP, DELL, *etc*. De ce fait, la maturité de cette technologie a donné naissance à une nouvelle génération des entreprises comme Facebook, Uber, AirBnB, *etc*., qui ne cessent de transformer le fonctionnement de plusieurs secteurs d'activités[(1)]. Toutes ces entreprises « *perturbatrices* » s'appuient principalement sur le Cloud Computing, c'est-à-dire, les clients accèdent à leurs services via Internet depuis n'importe quel endroit, à travers un appareil fixe ou mobile. Cependant, comme le souligne Farok Vakil, Victor Lu et Andrew Russakoff[(2)], le Cyber-État doit faire face à un nouveau phénomène appelé communément, « BYOD » (*Bring Your Own Device*, ou en français, Apportez vos appareils personnels). Ce changement de comportement des utilisateurs expose, dans le cadre du Cyber-État, les administrations publiques aux risques d'attaques informatiques et de perte de données confidentielles. Ainsi, aux risques du cyberespionnage et de la cybercriminalité.

A travers nos diverses recherches, nous constatons que l'émergence du Cloud Computing est en croissance continue. En effet, les années à venir présentent un terrain fertile à sa croissance et particulièrement avec le passage marquant du web 2.0[(3)] et ses réseaux sociaux au web 3.0[(4)] à base des objets connectés dans une économie de la donnée et une société hyper-connectée.

---

(1) L'entreprise *Uber* a transformé le métier des taxis dans le monde sans acquérir aucun taxi comme en témoigne les différentes manifestations des taxis parisiens en moi de Mai 2015. De son côté, l'entreprise américaine *AirBnB* bouleverse le secteur de l'immobilier sans posséder aucune agence immobilière. D'autres secteurs d'activités ont été impactés par la diffusion de ces applications en mode Cloud Computing comme les secteurs de voyage, de réservation d'hôtels, etc.

(2) F. VAKIL, V. LU et A. RUSSAKOFF, Recent Developments in Cloud Computing and High Speed Connections for Business Practices. Review of Business. 2012.

(3) L'expression « Web 2.0 » désigne l'ensemble des techniques, des fonctionnalités et des usages du web caractérisés par plus de simplicité et d'interactivité. Le web 2.0 concerne en particulier les interfaces permettant aux internautes ayant peu de connaissances techniques de s'approprier de nouvelles fonctionnalités du web.

(4) L'expression Web 3.0 est utilisée en futurologie à court terme pour désigner le Web qui suit le Web 2.0 et constitue l'étape à venir du développement du World Wide Web. Son contenu réel n'est pas défini de manière consensuelle, chacun l'utilisant pour désigner sa propre vision du futur d'internet.

c) Le Cloud Computing dans la littérature

A travers nos travaux de recherche, nous avons constaté que plusieurs travaux ont essayé de retracer un historique des définitions données pour le terme de Cloud Computing. En effet, ce travail a été principalement conduit Vaquero (2008), Etro (2011), Alali et Chia-Lun (2012). Nous avons trouvé que le terme Cloud Computing a été utilisé pour la première fois par par R.Chellappa (1997) alors que certains auteurs comme Sultan (2014) l'attribuent plutôt à Eric Schmidt, PDG de Google, lors d'une interview en 2006 dont voici un extrait :

> *« What's interesting [now] is that there is an emergent new model, and you all are here because you are part of that new model. I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it Cloud computing – they should be in a "cloud" somewhere. And that if you have the right kind of browser or the right kind of access, it doesn't matte*r».
>
> « *Ce qui est intéressant actuellement c'est qu'il y a un nouveau modèle qui émerge et vous êtes tous ici parce que vous en faites parties. Je ne pense pas que les gens ont bien compris l'ampleur de l'opportunité. Cela commence par mettre les données, les services les architectures dans des serveurs. Cela s'appelle le Coud Computing. Ils doivent être quelques part dans le « Cloud » et cela ne dépend pas de ton navigateur et de ton type d'accès* »

Pour certains auteurs comme Begin (2008), Buyya (2009), ou encore Abbadi et Martin (2010), la popularisation de Cloud Computing est due principalement au développement des entreprises américaines comme Amazon et Google.

A partir de notre découverte du terrain et notre analyse des différents entretiens avec des experts et spécialistes de Cloud Computing, nous constatons que toutes les personnes interrogées ne considéraient pas le Cloud Computing comme une révolution technologique marquant une rupture dans l'industrie informatique mais ils y voient plutôt une évolution technique basée sur un ensemble des notions déjà en place. Ils ont également soumigné le fait que le Cloud Computing ait largement profité d'un buzz marketing poussé par les grandes entreprises de l'industrie informatique. D'ailleurs, ce constat le confirme Larry Ellison, le PDG d 'Oracle, en déclarant à Wall Street Journal:

> « *The interesting thing about cloud computing is that we've redefined Cloud computing to include everything that we already do… I don't understand what we would do differently in the light of cloud computing other than change the wording of some our ads*». [(1)]

[(1)] Voir entretien complet sur le lien direct http://blogs.wsj.com/digits/2012/10/04/larry-ellison-says-he-invented-the-cloud/. Dernière consultation 18/10/2015 à 12h.

« *Le plus intéressant avec le Cloud Computing c'est que nous avons redéfini le terme pour inclure toutes les notions que nous connaissons déjà… Je ne comprends pas ce que nous pouvons faire différemment avec le Cloud Computing ce n'est que changer quelques mots dans nos publicités* ».

Nous mettons à disposition 'annexes la liste des définitions de Cloud Computing par auteur. Ainsi, à partir de cette liste, nous pouvons dresser une définition commune couvrant l'ensemble des aspects de « Cloud Computing» et qui reprend les différents points communs dans les différentes définitions :

- *Aspect 1* : Le Cloud Computing favorise un modèle « *service* » pour les clients. Le fournisseur des solutions Cloud Computing ne commercialise pas des composants mais plutôt un service prêt à être déployé (Plouin, 2011). Cette notion de service est systématiquement présente dans la totalité des définitions ;

- *Aspect 2* : Le service fourni se déploie à travers Internet ou via un réseau spécial dédié. Ce réseau est largement cité dans l'ensemble des définitions. Un réseau local entrepris (LAN) pourrait être utilisé mais cela reste marginal dans les définitions que nous avons pu trouver. Les auteurs faisant référence à l'utilisation d'Internet dans leurs définitions de Cloud Computing sont présentés ici dans un ordre chronologique d'apparition de leurs définitions : Armbrust (2009), Chen (2010), Haag et Cummings (2010), Katzan (2010), Shivakumar et Raju (2010), Nabil Ahmed (2011), David (2011), Espadas (2011), Lin et Chen (2012), Duta (2013), Gupta (2013), Ye (2013), Sultan (2013), Waxer (2013), Oliveira (2014).

d) Le Cloud Computing selon l'approche du National Institute of Standards and Technology (NIST)

Comme nous l'avons signalé dans l'introduction, à travers nos recherches, nous avons remarqué que la définition de *Cloud Computing* la plus répandue est celle donnée par le National Institute of Standards and Technology (NIST).

En effet, le NIST définit le Cloud Computing comme étant un « *modèle permettant d'offrir un accès simple, en tout lieu et à la demande, à un ensemble de serveurs informatiques configurables et partagés (par exemple : réseaux, serveurs, stockage, applications et services). Cet ensemble de ressources peut-être rapidement approvisionné et mis en service avec un minimum d'efforts de gestion et d'interventions du fournisseur*»[(1)].

[(1)] P. MELL et T. GRANCE, The NIST Definition of Cloud Computing, NIST, 2011, p.2.

Le plus important dans ce qu'il apporte la NIST est la grille de lecture du Cloud qui suit, avec ces éléments:

- Trois modèles de service : Software as a Service (SaaS), Plateforme as a Service (PaaS) et Infrastructure as a Service (IaaS) ;

- Quatre modèles de déploiement : Public, privé, hybride et communautaire ;

- Cinq caractéristiques : des services à la demande, des services mesurés, une bande passante élevée, un partage des ressources informatiques, et une élasticité et une flexibilité des ressources.

Le schéma[(1)] suivant reprend les différents éléments du modèle développé par le NIST :

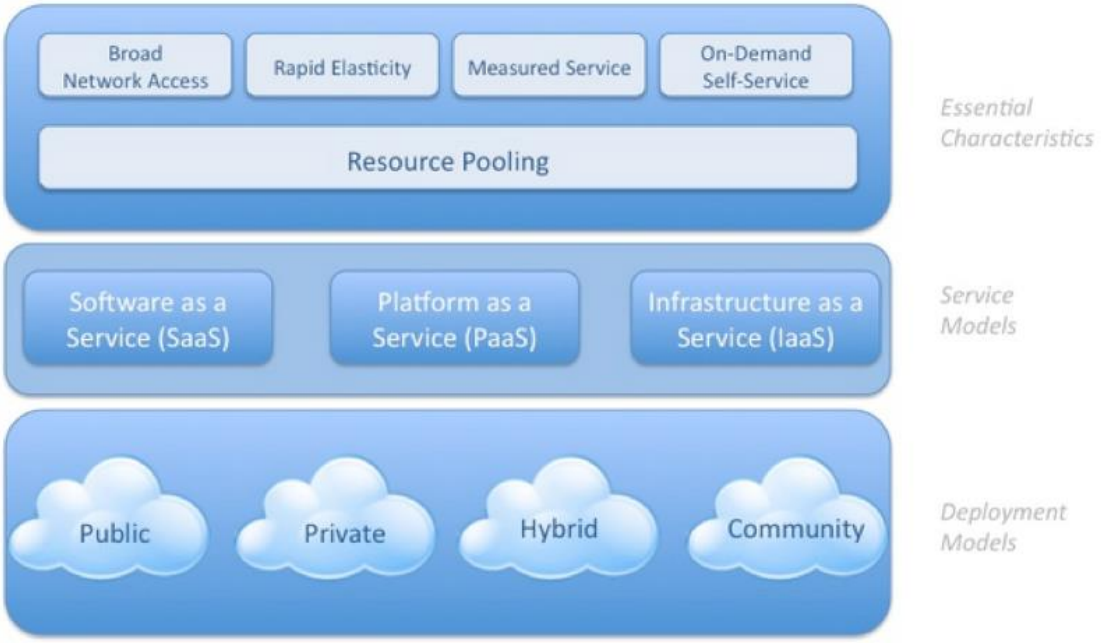


Figure 1 : Modèle de présentation du Cloud Computing par NIST

Afin de bien comprendre la technologie de Cloud Computing, nous allons détailler l'ensemble de ses éléments dans la suite de cette section.

---

(1) P. MELL ET T. GRANCE, The NIST Definition of Cloud Computing, NIST, 2011, p.2.

e) Approche NIST : Modèles de service

i. Le modèle SaaS – *Software as a Service*

Le modèle SaaS pour *Software as a Service* (logiciel comme service) permet de ne plus installer les applications sur ses propres serveurs informatiques mais plutôt de s'abonner à des services disponibles sur Internet en Cloud Computing.

Ainsi, le Software as a Service (SaaS), se réfère à tout service Cloud Computing permettant aux utilisateurs d'avoir accès à des applications logicielles sur Internet. Ces applications sont hébergées dans le Cloud Computing et peuvent être utilisées pour un large éventail de tâches, tant par les personnes privées que par les organisations. Google, Twitter, Facebook et Flickr sont tous des exemples des applications SaaS, où les utilisateurs peuvent avoir accès aux services via n'importe quel appareil disposant d'une connexion à Internet.

Ainsi, dans le cadre du Cyber-État, généralement, les citoyens utilisent des applications pour remplir de nombreuses tâches administratives, incluant la déclaration des imports, la facturation par les entreprises, le suivi des marchés publics, la planification des rendez-vous avec les administrations publiques, etc. Tous ces outils sont disponibles dans le Cloud Computing en mode SaaS.

ii. Le modèle PaaS – *Platform as a Service*

Platform as a Service (PaaS), est une catégorie de services de Cloud Computing qui fournit la plateforme et l'environnement informatique nécessaire aux développeurs pour mettre en place leurs différents services et applications sur Internet. Les services PaaS sont hébergés dans le Cloud et les utilisateurs y accèdent simplement, par leur navigateur web (Internet Explorer ou Mozilla Firefox, etc).

Les services PaaS permettent aux utilisateurs de créer des applications logicielles en utilisant les outils fournis par le fournisseur Cloud Computing. Ils peuvent prendre la forme de fonctionnalités préconfigurées auxquelles les clients peuvent souscrire, en ne choisissant que celles qui conviennent à leurs exigences.

Comme avec la plupart des offres Cloud Computing, les services PaaS sont facturés sur la base d'un système d'abonnement, où les utilisateurs ne paient que ce qu'ils utilisent effectivement. Les utilisateurs bénéficient également des économies d'échelle tirées du partage des infrastructures physiques existantes entre les utilisateurs.

Ainsi, le modèle PaaS fournit un environnement d'exploitation pour le développement d'applications. En d'autres mots, il fournit l'architecture et l'infrastructure globale nécessaire pour supporter le développement d'applications. Cela inclut le réseau, le stockage, le support logiciel et les services de gestion.

iii. Le modèle IaaS – *Infrastructure as a Service*

L'Infrastructure *as a Service* (IaaS) est l'une des trois principales catégories de services de Cloud Computing, avec Software as a Service (SaaS) et Platform as a Service (PaaS).

Comme pour tous les services de Cloud Computing, ce service donne accès aux ressources informatiques distantes dans le Cloud Computing, à travers une connexion Internet. Ainsi, dans le cas de l'IaaS, la ressource informatique fournie est une infrastructure informatique. La définition du service comprend des offres telles que l'espace serveur de stockage, des connections réseaux, des adresses IP, des logiciel de sécurité informatiques, *etc*.

A l'instar des deux autres formes de Cloud Computing, l'IaaS peut être utilisée par les utilisateurs pour créer des solutions informatiques à des coûts très bas. Les ressources informatiques louées sont facilement extensibles, dans la mesure où la complexité et les coûts inhérents à la gestion du matériel informatique sont pris en charge par le fournisseur de la solution Cloud Computing.

f) Approche NIST : Modèles de déploiement

i. Déploiement Cloud Privé

Un Cloud Privé est un modèle de Cloud Computing constitué par un environnement Cloud distinct et sécurisé auquel l'accès est dédié à seul un client. Ainsi, dans ce modèle du Cloud, l'accès n'est accessible que par une seule organisation, lui donnant ainsi davantage de contrôle, de protection et de confidentialité de ses propres données.

Les deux caractéristiques du Cloud Privé sont la délimitation d'un Cloud pour l'utilisation d'une seule organisation ainsi qu'un degré plus élevé de sécurité du réseau. Ainsi, le Cloud Privé se distingue du Cloud Public, dans lequel de nombreuses organisations accèdent à des services hébergés dans des ressources partagées à travers des réseaux publics.

La sécurité supplémentaire que fournit le modèle de Cloud Privé est adaptée à tout type d'organisation ayant besoin de stocker et de traiter des données privées, ou alors d'exécuter des tâches sensibles. Par exemple, un service de Cloud Privé peut être utilisé par une société financière obligée par la législation en vigueur de stocker des données sensibles internes, mais qui souhaite également avoir recours à certains avantages du Cloud Computing dans son infrastructure informatique.

Ainsi, le Cloud Privé étant accessible seulement par une organisation déterminée, cette dernière a la possibilité de le configurer et de le gérer selon ses besoins. Cependant, un tel niveau de contrôle supprime certaines économies d'échelle rendues possibles par le fait d'avoir choisi de migrer une partie de son système informatique dans le Cloud.

ii. Déploiement Cloud Public

Le modèle de Cloud public est le plus connu des modèles Cloud Computing. Les services sont fournis dans un environnement construit en utilisant des ressources physiques partagées entre plusieurs organisations et accessible via un réseau public, Internet. Les services de Cloud Public peuvent être définis par opposition au Cloud Privé, auquel une seule organisation spécifique peut avoir accès. En revanche, le Cloud Public fourni des services à des clients multiples en utilisant la même infrastructure partagée

Le Cloud Public rassemble de plus grandes quantités de ressources afin de pouvoir bénéficier de vastes économies d'échelle. L'exploitation et la gestion centralisées des ressources sont partagées entre tous les services Cloud alors que les composants, comme les serveurs, nécessitent moins de configuration personnalisée. Ainsi, les services de Cloud Public utilisent souvent un modèle de tarification basée sur l'utilisation, selon lequel le consommateur peut accéder aux ressources dont il a besoin, quand il en a besoin, et ne paie que ce qu'il a effectivement consommé, évitant ainsi un gaspillage de capacités.

D’un point de vue sécurité, le Cloud Public assure une sécurité physique. En effet, la grande quantité de serveurs et de réseaux impliqués ainsi que les configurations redondantes signifient qu'en cas de panne de l'un des composants, le Cloud continue à fonctionner sur les autres composants. Cependant, vu que toutes ces ressources sont partagées entre plusieurs organisations, ce modèle représente un risque réel pour la confidentialité des données, par conséquent, c’est un modèle qui convient à des services non critiques.

iii. Déploiement Cloud Hybride

Un Cloud hybride est un service Cloud intégré utilisant à la fois un Cloud Privé et un Cloud Public pour remplir différentes fonctions au sein d'une même organisation.

En effet, si tous les types de services Cloud sont sensés offrir un certain niveau d'efficacité, à des degrés divers, les services Cloud Public sont susceptibles d'être plus avantageux au niveau des coûts et plus évolutifs que les Cloud Privé. C'est pourquoi une organisation peut maximiser son efficacité en utilisant des services de Cloud Public pour ses opérations non-sensibles et s'appuyer en revanche sur un Cloud Privé pour toutes ses tâches critiques, faisant en sorte que toutes ses plateformes soient intégrées harmonieusement.

Le modèle de Cloud Hybride peut être mis en œuvre de nombreuses façons :

- Différents fournisseurs de Cloud s'unissent afin de fournir des services intégrés en Cloud Privé et Public ;
- Des fournisseurs de Cloud Privé proposent un hybride complet ;
- Les organisations gérant elles-mêmes leur propre Cloud Privé souscrivent à un service de Cloud Public qu'elles intègrent ensuite dans leur infrastructure.

Par exemple, une entreprise peut mettre en place un hébergement Cloud Hybride pour héberger son site web de commerce électronique dans un Cloud Privé, sécurisé et évolutif et héberger son site web ordinaire dans un Cloud Public, plus avantageux en termes de coûts (car la sécurité est moins importante dans ce cas).

iv. Déploiement Cloud Communautaire

Ce type de modèle Cloud Communautaire comme son nom l’indique, permet aux entités ayant des préoccupations similaires, de partager leurs ressources informatiques. Ces ressources informatiques peuvent être gérées par une ou plusieurs entités membres de la communauté, ou alors externalisées, gérées par un tiers.

Cependant, faire appel à ce type de déploiement est très rare et peut être trouvé seulement au sein des entités d’un même groupe.

g) Approche NIST : Caractéristiques des services

i. Services à la demande

La caractéristique « à la demande » signifie que les clients peuvent adapter leurs demandes à la hausse comme à la baisse selon les évolutions de leurs besoins. En effet, cette caractéristique signifie que les clients puissent s'abonner aux services à travers Internet sans passer par des intermédiaires ou des revendeurs. Chaque client pourrait avoir une interface pour bien gérer son abonnement.

ii. Services mesurés

Les fournisseurs des solutions Cloud sont capables de mesurer de façon précise la consommation des différentes ressources informatique : CPU, Stockage, bande passante…); Ces indices permettent d'établir une facturation pour le client selon sa consumation.

iii. Accessible sur l'ensemble du réseau

Les solutions Cloud s'appuient obligatoirement sur le réseau (internet) et est accessible via le réseau, quel que soit le périphérique (PC, Mac, TV, Tablette, Smartphone)

iv. Mutualisation des ressources informatiques

Dans un environnement Cloud, les ressources informatiques sont souvent mutualisées afin de réduire les couts d'exploitation et de maintenance.

v. Élasticité et une flexibilité des ressources.

Le Cloud Computing permet une élasticité et une flexibilité d'apprivoisement des ressources informatiques. En effet, il est possible de disposer de plus de ressources très rapidement pour soutenir une forte demande ou pour absorber un pic d'activité. Il est également possible, dans le sens inverse, de réduire ses ressources si l'activité baisse et ne justifie la mobilisation de toutes ces ressources.

h) Etude de cas démonstrative: Adoption de Cloud Computing

Pour montrer l'apport du Cloud Computing pour une entreprise, nous reprenons certains éléments de l'étude de cas que nous avons publié dans Harvard Business Review[(1)] et qui démontre comment le Cloud Computing pourrait améliorer la compétitivité des moyennes entreprises comme cas d'étude.

D'abord notons que les PME représentent une composante essentielle de l'économie nationale. Elles se caractérisent par leurs capacités de résilience, d'investissement continu et d'innovation (un tiers des brevets est détenu par les PME, selon l'observatoire de la propriété intellectuelle). Elles peuvent améliorer leurs performances en faisant appel à des services disponibles dans le Cloud. Selon une étude(24) réalisée par Microsoft, 59% des PME, consommatrices de ce type de services, ont constaté une croissance de leur productivité. En effet, les services Cloud offrent plusieurs avantages aux PME et déchargent ces dernières des contraintes liées à la gestion de l'informatique. Ce constat est confirmé par l'étude de KPMG citée plus haut. Les services Cloud les plus sollicités par les entreprises interrogées sont ceux de la gestion des ressources humaines (57%), de la gestion de l'infrastructure IT (54%) et des outils de collaboration (53%). D'une manière générale, les entreprises font appel aux services suivants dans le Cloud :

- Les outils de productivité et de collaboration : messagerie électronique (e.g. la suite Office 365), réseaux sociaux d'entreprises (e.g. Yammer) ;
- Les sites Internet : portail intranet entreprise, sites web, etc ;
- Les services de stockage et de partage en ligne ;
- Les applications métier : Gestion de la relation client (CRM), gestion des ressources humaines (GRH), etc.

Néanmoins, la migration des services vers le Cloud représente des risques liés principalement :

- Aux problématiques de confidentialité des données ;
- A la fiabilité des fournisseurs du Cloud ;
- A la capacité de migration d'un fournisseur vers un autre, avec une reprise de l'historique des opérations.

---

(1) Etude disponible directement sur http://www.hbrfrance.fr/chroniques-experts/2015/01/5779-comment-le-cloud-peut-il-booster-la-competitivite-des-pme, dernière consultation 20/08/2015, à 11h30.

Afin d'illustrer l'apport d'un service Cloud pour une PME, prenons l'exemple de la mise en place d'un service de stockage des données métier : factures clients, fiches fournisseurs, etc.

Selon le modèle d'implémentation choisi par la PME, la mise en place de ce service de stockage implique les opérations suivantes :

Solution dite « *On premise* » ou locale	**Solution dans le Cloud**
– Achat du matériel (Hardware) et des licences logicielles associées (Software) – Charges d'exploitation et de maintenance : mise à jour, sauvegarde, etc. – Une équipe technique compétente pour gérer cette infrastructure : technicien système par exemple – Rigidité : Si le besoin en termes de stockage augmente, il serait nécessaire de renforcer les ressources techniques et humaines	– Souscription à un service Cloud de stockage : Sharepoint de Microsoft par exemple – Le fournisseur prend en charge l'exploitation et la maintenance de la solution avec un support 24x7 – Flexibilité : La PME peut augmenter ou réduire les ressources selon ses besoins et payer selon sa consommation – La PME se décharge de cette activité technique et se concentre sur son métier

Tableau 2 : Comparaison des deux solutions d'hébergement : Cloud et On-premise [(1)]

Nous remarquons qu'avec l'option Cloud :

- La PME loue le service au lieu d'acheter une solution propre. Elle contribue ainsi à transformer le capital en dépenses opérationnelles variables (Opex (*Operational expenditure*), par opposition au Capex (*Capital expenditure*)) ;
- Le fournisseur est le responsable du service complet : mise en place, configuration, maintenance, etc. Ainsi, la PME n'a plus à se charger de la gestion technique ;
- La PME gagne en flexibilité et en rapidité de mise en place ;
- La PME peut améliorer sa stratégie «*Go-to-Market*».

---

(1) Tableau réalisé par nous-même d'après notre compréhension du sujet. Tableau non issu d'aucune source bibliographique

B. Le Cloud souverain à l'ère du Cyber-État : un défi dans le cadre dépendant de la sécurité nationale ?

Le mot souverain, adjectif, du latin populaire *superanus* et du latin classique *superus*. Le mot souverain est synonyme de suprême.

Le terme souverain peut avoir plusieurs significations dans le domaine politique, administratif et juridique. En effet, il peut signifier celui qui détient la souveraineté et qui exerce le pouvoir sur un territoire si nous parlions d'une personne. Ou bien qui se gouverne soi-même tout en pouvant relever d'une autorité supérieure si nous parlions d'une collectivité politique. En parlant d'un État, il signifie celui qui a la souveraineté interne et externe. Si nous parlions d'une institution, le mot souverain signifie une institution dont les actes, les décisions sont sans appel. En parlant d'une chose sans marque particulière, le mot signifie qui est au plus haut degré qui règne en maître, l'emporte sur les autres, qui excelle dans son genre, dans son domaine.

Ainsi, à partir de ces éléments, nous pouvons proposer une définition du cloud souverain comme étant l'outil technologique qui va donner la capacité au Cyber-État d'assurer sa cybersouveraineté dans un environnement cyberspace.

Cependant, seuls Cloudwatt et Numergy représentent le cloud dit souverain en France. Avant leur apparition, ils préexistaient de nombreux cloud dits « français », de OVH à Ikoula et bien d'autres. Cependant, la particularité de ces deux Clouds dits « souverain » est la participation de l'État dans leur financement. En effet, Numergy et Cloudwatt sont financés par l'État dans le cadre du « Grand Emprunt » ou « investissement d'Avenir(1). Par l'intermédiaire de la Caisse des dépôts et consignations, l'État entre ainsi à hauteur de 33,3 % au capital de Cloudwatt, dont les autres actionnaires sont Orange (44,4 %) et Thales (22,2 %). Quant à Numergy, le capital se répartit entre SFR (47 %), Bull (20 %) et la Caisse des dépôts (33 %). L'État possède donc la minorité de blocage dans les deux structures.

---

(1) Les investissements d'avenir (appelés un temps « grand emprunt ») est un programme d'investissement de l'État français, débuté en 2010 et toujours en cours en 2015. L'ensemble des opérations mobilise 47 milliards d'euros, 35 milliards programmés par le gouvernement Fillon auxquels se sont ajoutés 12 milliards par le gouvernement Ayrault. Ces fonds ont permis, entre autres, un soutien à la recherche et aux projets innovants, la création des instituts de recherche technologique (IRT), des Institut hospitalo-universitaire (IHU), des sociétés d'accélération du transfert de technologies (SATT) et un soutien au projet de cluster technologique Paris-Saclay.

En effet, suite au Patriot Act et aux révélations d'Edouard Snowden, la France, comme bien d'autres pays, ont décidé de construire leur propre cloud. En 2009, le gouvernement François Fillon a lancé un projet de cloud « souverain », destiné aux administrations mais aussi aux entreprises privées. Ce cloud souverain devait servir à stocker des informations sensibles telles que des données personnelles administratives, des renseignements liés à l'e-santé ou encore des informations économiques nécessitant un maximum de sécurité.

> « *Il faut absolument que nous soyons capables de développer une alternative française et européenne dans ce domaine, qui connaît un développement exponentiel, que les Nord-Américains dominent actuellement*.» [(1)]
> (*François Fillon, premier ministre 2007 -2012*).

Ainsi ce projet de Cloud souverain apporte des réponses aux enjeux de localisation des données. En effet, les deux projets Cloudwatt et Nuergy sont principalement hébérgé en France comme le montre le tableau ci-dessous. Ainsi, la souveraineté de la donnée hébergée dans ces centres de donnée est assurée loin des pratiques du Patriot Act. Cependant, une bonne sécurité des données dans le cloud implique une connaissance de l'architecture technique du centre des données hébergeant le Cloud, une connaissance du territoire où il se localise ce centre de données, une vérification des accès au site et aux locaux, une bonne maitrise de l'énergie et de la climatisation ainsi qu'une connaissance interne et externe de l'organisation des sites de production. Ainsi, le Cloud souverain semble apporté des réponse à l'ensemble de ses questions comme en témoigne les déclarations du président directeur général du Numergy:

> « *Si l'on compare notre activité avec celle d'un fournisseur d'électricité, on peut dire qu'on est comme EDF ; et si l'on regarde les fournisseurs de carburants, on est comme Total, Elf, etc. […] on ne construit pas les véhicules, ni les ampoules* ». [(30)]
> (Président Directeur Général Numergy)

Dans le cadre de notre découverte du terrain, nous avons pu rencontrer le directeur technique de Numergy, avce qui nous avons discuté sur les éléments techniques qui pourront assurer une sécurité absolue du cloud souverain.

[(1)] Cité dans La Tribune, 13/01/2015, lien direct: http://www.latribune.fr/technos-medias/informatique/20150113triba29598d73/le-cloud-a-la-francaise-histoire-d-un-flop.html, dernière consultation 20/08/2015 à 14h.

[(2)] Cité par Franck Leon. La construction des Business Models des fournisseurs de services d'infrastructure Cloud Computing (IaaS). Business administration. Université Nice Sophia Antipolis, 2015.

C. Vers des référentiels de confiance dans le Cloud

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est créée le 7 juillet 2009. Elle remplace le Chiffre de la période de la guerre froide et dépend aujourd'hui du Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) créé en 2008 sous l'autorité du Premier ministre dont les missions ont été définies dans les Livres Blancs de la Défense et de la Sécurité Nationale (LB) de 2008 et de 2013.

ANSSI a publié en 2014 un appel public à commentaires sur un référentiel applicable «aux prestataires de services sécurisés d'information en nuage ». Ce document dresse un inventaire des bonnes pratiques dans le domaine de la sécurité et du Cloud Computing.

Ainsi, un référentiel n'est pas une norme juridique. En effet, le non-respect d'un référentiel n'est pas susceptible d'une sanction prononcée par un tribunal. Le référentiel, qu'on peut encore appeler recommandation ou guide de bonnes pratiques, est une liste de points que des experts invitent à respecter. Le référentiel est plutôt un document pédagogique ou didactique, censé apporter un savoir-faire, une connaissance à des lecteurs professionnels. Les référentiels peuvent émaner de personnes publiques, comme c'est le cas avec l'ANSSI. Par exemple, depuis sa création en 1978, jusqu'en 2004, la Commission Nationale de l'Informatique et des Libertés (CNIL) ne disposait que de recommandations pour faire valoir un point de vue tranché, avant qu'elle n'acquière un pouvoir de sanction. Au niveau international, une norme ISO est en cours d'élaboration, qui touche également à la sécurité et au Cloud, dont le statut juridique est identique au référentiel en cours d'élaboration par l'ANSSI.

Malgré que le référentiel ne soit pas une norme juridique à respecter cependant son pouvoir d'influence est très important. En effet, dans un rapport publié par le Conseil Economique, Social et Environnemental en Janvier 2014 sur la gouvernance d'Internet, on pouvait lire au chapitre cybercriminalité, le texte suivant : « *l'annonce de cyberattaques ponctue régulièrement l'actualité et si leur nombre s'accroît, c'est surtout leur hyper-sophistication qui frappe les esprits (...) Or dans les faits, il s'avère souvent impossible d'identifier et de poursuivre les coupables*. ». Ainsi, pour face à la cybercriminalité et être capable de suivre et de déterminer les responsables, un prestataire Cloud qui se sera engagé au respect d'un référentiel et pourra prouver qu'il s'y est conformé, verra le risque de responsabilité s'éloigner.

Ainsi, comme le montre Gabriel Péries, l'ANSSI, vérifie la procédure d'habilitation qui vise à s'assurer de « la conformité de l'organisme aux critères de qualité et de technicité selon les règles et normes d'accréditation en vigueur » et de « la compétence technique de l'organisme à conduire l'évaluation de fonctions de sécurité mises en œuvre par un prestataire de services de confiance (PSCO) au regard des règles du référentiel général de sécurité (RGS) » dans le cadre de la doctrine de la sécurité nationale (DSN) depuis que l'État français a réintégré le commandement SHAPE de l'OTAN.

D. Quel Cloud Computing pour l'État marocain ?

En réponse au *Patriot Act*, comme c'est le cas pour la France, le gouvernement marocain a organisé, en partenariat avec Microsoft Afrique, un sommet national pour réfléchir sur une stratégie nationale de développement d'un Cloud souverain pour répondre aux différentes problématiques liées à l'hébergement des données critiques de l'État marocain ainsi faire face aux programmes d'espionnage étranger.

Ainsi, l'événement a réuni des décideurs des milieux économiques et politiques marocains , notamment Latifa Echihabi, secrétaire Général du ministère de l'Industrie, du Commerce, de l'Investissement et de l'Economie numérique et Boubker Badr, Directeur de l'Economie Numérique, autour des nouvelles contraintes numériques dont ils font face les services gouvernementaux et les administrations publiques au Maroc.

Ainsi, Les collectivités locales et les administrations publiques marocaines vivent aujourd'hui dans un contexte de forte pression budgétaire et doivent en même temps offrir davantage de services et d'interactivité aux citoyens. Ces derniers adoptent de plus en plus des outils numériques et s'attendent que l'État puisse proposer également des services du même niveau de qualité.

Durant notre découverte du terrain, nous avons pu rencontrer le responsable technologique de Microsoft Maghreb. Ainsi, il précise que :

> *« La mise en place d'une stratégie moderne de Cloud National doit combiner de manière intégrée un Cloud gouvernemental marocain pour héberger certaines données et applications directement sur le territoire marocain, via la mise en place de datacenters aux normes internationales, et des Cloud publics internationaux qui offrent de très grandes capacité à des coûts très faibles, ce qui permet de répondre à des besoins précis qui ne sont pas sensibles du point de vue de la sécurité nationale. Ces Clouds publics peuvent également desservir des pays voisins en Afrique … En Europe, Microsoft étend chaque année ses capacités d'hébergement informatique sur le continent. Rien qu'en Irlande, nous venons d'investir 170 millions d'euros dans une extension de notre datacenter. C'est plus de 15 700 m2 de surface d'hébergement supplémentaires qui seront ouverts au printemps 2014, soit une capacité d'hébergement totale de 54 255 m2. Ces investissements s'expliquent par l'accroissement de la demande en Europe, au Moyen-Orient et en Afrique pour nos services Cloud public comme Office 365 ou Windows Azure. De plus, nous accompagnons plusieurs gouvernements et partenaires privés dans la mise en place de Clouds nationaux en apportant notre expérience et les solutions que nous utilisons pour construire et gérer nos propres Clouds »*[(1)].

[(1)] déclarations apparues dans le communiqué de presse de la frime américaine Microsoft, disponible sur le lien : https://news.microsoft.com/fr-xf/2013/12/12/microsoft-maroc-lance-la-1ere-edition-du-national-cloud-summit-et-promeut-le-cloud-national-pour-le-gouvernement-et-les-administrations-publiques-afin-de-reduire-les-couts-et-daugmenter-l/ (dernière consultation : 03/09/2016 – à 00h30)

En effet, cette réflexion du gouvernement marocain a abouti à un projet de création d'un Cloud souverain au Nord du pays (voir carte du Maroc ci-dessous) pour des besoins critique de l'administration marocaine. Ce projet, malgré sa confidentialité, nous a été confirmé également dans un entretien avec le président de la Commission Nation de protection des données personnelles au Maroc lors d'un entretien qui s'inscrit toujours dans la découverte du terrain de recherche.



Figure 13 : Carte officielle du Maroc issue de http://www.sahara.gov.ma/

E. Plan industriel Cloud Computing

a) Contexte

La nouvelle France industrielle est le nom donné aux plans de ré industrialisation de la France mis en place par le gouvernement français et présentés le 12 septembre 2013 par le président François Hollande et Arnaud Montebourg, ministre du Redressement productif (2012-2014). A travers ce plan stratégique, le gouvernement français a défini 34 plans industriels dont le plan Cloud Computing.

Ainsi, sur la base de différents travaux supervisés les acteurs suivants :

- Les écoles et Organismes de recherche public est particulièrement l'Institut National de Recherche en Informatique et en Automatique (INRIA) ;
- Les acteurs publics comme Banque Publique d'Investissement (BPI), Chambre Général d'Industrie (CGI), Ministère de l'Économie, du Redressement Productif et du Numérique (2012-2014) ainsi que la Direction Générale des Entreprises (DGE) ;
- Les acteurs industriels français comme Atos, OVH, Bull, Orange, Numergy, Cloudwatt, Axway, etc.

Ainsi, la feuille de inclut 10 propositions visant à accélérer l'émergence d'alternatives françaises en matière de Cloud Computing. Ainsi, ces propositions peuvent être distinguées en deux catégories : Mesure en faveur de la demande et des mesures en faveur de l'offre. Nous allons donc détailler les deux propositions.

b) Des mesures en faveur de la demande (pour les particulier)

- ***Création d'un label sécurité « Secure Cloud » pour les offres de Cloud Computing*** :
  Cette labellisation à vocation européenne pour les acteurs hébergeant et traitant les données sur le territoire européen selon des normes contractuelles de qualité et de sécurité élevées.

- ***Exemplarité de l'action publique et création d'une place de marché numérique pour les collectivités locales***.
  Ainsi, le passage au Cloud de l'informatique de l'État, des organismes publics et des collectivités locales et création d'un guide de bonnes pratiques ; création de «places de marché cloud » proposant des applications validées et sécurisées pour les collectivités locales (puis, plus largement, les entités publiques) ;

- ***Neutralité Cloud dans les marchés publics.***
  Ainsi, le groupe du travail insiste sur la mise en place de procédures de marché public assurant une neutralité vis-à-vis des offres Cloud ;

- ***Adoption du Cloud par les entreprises (aide à la transformation numérique).***
  Ainsi, il faudra amplifier l'accompagnement des entreprises, et notamment des PME, vers le Cloud et la création ou l'extension de relations numériques avec leurs clients ;

- ***Adoption du Cloud par le grand public (« cloud personnel* »).**
  Le groupe insiste sur le lancement d'une initiative autour des domaines personnels pour permettre à chaque français de disposer de son nom de domaine à faible coût, de la gestion d'identité numérique, des espaces de stockage personnels sécurisés, etc.

c) Des mesures en faveur de l'offre (pour les industriels)

- ***Garantir un traitement sécurisé des données en Europe.***
  En effet, le groupe du travail préconise la mise en place des normes élevées de qualité et de sécurité ainsi que la mise en place de règles harmonisées de qualité de service et de protection des données au niveau européen ;

- **Augmenter l'attractivité de la France pour l'installation et la construction des centres de données (datacenters)**
  en simplifiant les démarches administratives de création ainsi que des mesures fiscales d'encouragement.

- ***Aide aux éditeurs de logiciels à la transition vers le Cloud***
  par la création d'une « plate-forme tremplin » globale permettant la transformation Cloud des offres des acteurs de l'informatique et notamment des éditeurs de logiciels ;

- ***Soutien à l'innovation dans le cloud***
  Avec une orientation d'usage et de soutien à des projets visant à développer des services Cloud correspondant aux besoins de communautés d'utilisateurs (éducation, santé, seniors, etc.) ;

- ***Renforcer les formations Cloud*, l'attractivité et l'organisation de la filière**
  Via le développement de cursus en formation initiale et continue, s'appuyant sur des méthodes pédagogiques issues du numérique ainsi que contribution à l'attractivité des métiers, et création d'un «observatoire du Cloud»

3. Chapitre 3 : Fondements techniques du Cyber-État : Big data

L'objectif de cette section est de comprendre, techniquement et fonctionnellement, la technologie de Big data. .

En effet, à travers cette section, nous présenterons l'ensemble des définitions de ce terme et ses différentes caractéristiques. Nous présenterons le métier de « data scientist » ainsi que son rôle dans le secteur public. Nous terminerons par une présentation des outils techniques utilisés par les technologies Big data ainsi que les différentes initiatives de l'État français et marocain en matière de Big data.

Les thèmes principaux traités sont :

- Présentation de la technologie de Big data ;
- La fonction de « Chief Data Office » dans le cyber-secteur public ;
- Les outils du Big data ;
- Le plan Big data (Nouvelle France industrielle) ;
- La mission Etalab (Opendata).

A. Big data comme fondement technique du Cyber-État

a) Définition du Big data

Selon les deux auteurs Brynjolfsson et McAfee (2011), le boom du « Big Data » constituerait l'innovation de notre époque. Une innovation dont les effets impacteront tous les domaines, allant de la science à la recherche, en passant par le monde des affaires et la gestion des services gouvernementaux et le monde des arts (The Economist, 2010)[(1)]. Pour d'autres comme Chris Anderson (Wired, 2008)[(2)] , non seulement nos capacités à répondre aux questions fondamentales progressent à mesure que s'accroissent les faits, mais le « Big data » rendrait même à toute fin utile obsolète la méthode scientifique traditionnelle.

Comme le fait remarquer Lev Manovich (2011), le terme « Big Data » est mal adapté. En effet, ce terme a été utilisé en sciences pour faire référence à des ensembles de données suffisamment grands pour nécessiter l'utilisation de superordinateurs, alors que de vastes ensembles de données peuvent désormais être analysés sur des ordinateurs classiques en utilisant des logiciels standards. Par ailleurs, la nouveauté du Big Data ne réside pas seulement dans la quantité des données produites chaque jour par les individus, les organisations et les objets mais plutôt dans leurs capacités à être articulées à d'autres données. En raison des efforts pour exploiter et agréger les données, les « Big Data » sont fondamentalement liées aux réseaux. Leurs valeurs viennent des «patterns » qui peuvent être tirés du fait de connecter entre eux des jeux de données, concernant un individu, des individus liés à d'autres, des groupes de gens, ou simplement concernant la structure de l'information elle-même.

---

(1) voir The Economist, « *Data, Data Everywhere. Special Report : Managing Information* », The Economist, 25 février 2010.

(2) voir Wired, 2008, *http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory* , dernière consultation (08 Mai 2015).

b) Caractéristiques du Big data

Depuis le début de l'informatique personnelle dans les années 1980s, l'internet des années 1990s, puis le web 2.0 des années 2000s et l'arrivée du web 3.0 dans les années à venir, les données ont été produites en quantité avec une constante croissance. Toutes ces données sont sous formes des articles, blogs, vidéos, photos, données géographiques, … Suite à la démocratisation de l'Internet, des grandes quantités de données sont produites chaque jour par les individus et des organisations. A titre d'exemple, le site Planetoscope[(1)] a estimé à 3 millions le nombre des e-mails envoyés dans le monde chaque seconde, soit plus de 200 milliards par jour dont 90% de spams, et ce pour 40% de la population mondiale connectée sur Internet.

Ce déluge d'information n'est pas seulement imputable à l'activité humaine mais de plus en plus à des objets et des machines connectés qui contribuent à la génération de ces volumes de données : on parle alors des Internet des objets (Internet Of Things).

Comme nous l'avons vu dans la partie introductive, le terme « Big data », se traduit littéralement par « grosses données » ou « données massives », désigne l'explosion de la production des données à l'ère numérique. En consultant la littérature scientifique, on se rend compte de la multiplicité des définitions souvent tournées autour des trois «V » : Volume, Vélocité et Variété. En effet, ces 3 caractéristiques ont été initialement proposées par les spécialistes d'IBM. Par la suite, d'autres experts ont ajouté d'autres caractéristiques en « V » en complétement des 3V cités précédemment afin de couvrir toutes les caractéristiques d'un phénomène « Big data ». Les 6 caractéristiques en « V » sont les suivantes :

- ***Volume*** :
  la quantité de données générées va continuer à augmenter de manière exponentielle à l'ère des médias sociaux et des objets connectés;

- ***Vélocité*** **ou encore Vitesse :**
  Ces données massives sont générées de plus en plus rapidement et en flux continu. Leur analyse nécessite de plus en plus le temps réel ;

- ***Variété*** **:**
  Ces données se présentent dans de différents formats (texte, image ou son, etc.). Ils peuvent être structurées, semi-structurées ou encore non-structurées ;

---

(1) Voir, Planetoscope.com pour plus des informations à jour. Dernière consultation 29/08/2015 à 12h.

- ***Variabilité*:**
  Ces données sont de nature variable c'est-à-dire elles peuvent être changeables et interchangeables au fil de l'eau ;

- ***Véracité* :**
  Ces données entrant dans des cycles de traitement, leur qualité, authenticité et exactitude sont primordiales ;

- ***Valeur*** :
  Celle-ci peut être tangible (monnayable) ou non mais toujours appréciable d'une manière ou d'une autre au regard de la performance organisationnelle.

B. La fonction de « Chief Data Officer » à l'ère du Cyber-État

a) Contexte

Comme nous l'avons mentionné dans la section 1, la fonction publique va être évoluée avec l'émergence de Cyber-État. Ainsi, des nouveaux métiers, certes hautement qualifiés, viendront remplacer d'autres fonctions qui vont disparaitre dans le service public. Ainsi, l'administrateur général des données, communément connu sous le *Chief Data Officer*, fait partie de ces nouveaux métiers de la fonction publique.

Ainsi, l'administrateur général des données va contribuer à la qualité des données produites par le Cyber-État. Il va faciliter la circulation des données au sein de l'administration comme à destination des chercheurs, entreprises et citoyens et principalement à travers des missions de « cyber-service public ». Entre autre, il est responsable de la production de données clés pour appuyer des politiques publiques et des cyber-politiques publiques. Il doit également stimuler la diffusion au sein des administrations publiques, des nouvelles méthodes du travail fondées la donnée.

D'un point de vue sécurité et sécurité nationale, il est l'interlocuteur privilégié en matière d'interprétation des grandes masses de donnés produites dans le cadre de la mise en place de différentes relatives à assurer la sécurité nationale : Loi de programmation militaire, loi anti-terroriste ainsi que la loi relative au renseignement. Ainsi, les algorithmes des boites noires installées chez les opérateurs télécoms et les Fournisseurs d'Accès Internet (FAI) doivent être sous sa responsabilité ainsi s'assurer de leur conformité aux différentes législations.

Il doit également appuyer les positions de la France dans les négociations internationales en matière de protection des données personnelles et travailler avec ses homologues européens pour définir un cadre commun de traitement des données ainsi définir une stratégie nationale et européenne en matière de la donnée.

Enfin, il est autorisé à conduire des expérimentations sur l'utilisation des données pour renforcer l'efficacité des politiques publiques, contribuer à la bonne gestion des deniers publics et améliorer la qualité des services rendus aux citoyens.

L'administrateur général des données est assisté dans son travail par une équipe de « data scientists » dont nous allons voir les différentes caractéristiques.

Nous signalons qu'aujourd'hui nous n'avons pas trouvé des initiatives au Maroc faisant référence à la création d'un tel poste au sein de l'administration marocain.

b) Définition du «data scientist»

Le «*data scientist*» (ou scientifique de données en français) est un métier récent qui est apparu ces dernières années dans le sillage du Big data. De nombreux débats ont lieu sur sa définition, ses compétences, sa différence par rapport à un statisticien ou un analyste mais également par rapport à la place qu'il peut occuper au sein des organisations. Certains spécialistes le voient comme une tendance passagère dans l'informatique alors que d'autres spécialistes; au contraire; y voient un nouveau métier d'avenir qui émerge.

Le terme de «*data scientist*» s'est fait connaitre en 2008 après la publication dans Harvard Business Review (HBR) de l'article « *Data scientist : The sexiest job of 21st century* »[(1)]. Et depuis, ce métier a gagné de l'importance et est devenu indispensable pour l'analyse et l'exploitation des données au sein des grandes organisations. Cependant, les compétences nécessaires d'un tel profile sont rares comme ce fut le cas; à une époque; pour les analystes financiers dans les années 1980s et 1990s à Wall Street.

Le métier de «*data scientist*» est donc né dans un contexte d'évolution des technologies innovantes comme le Big data. Il doit savoir en tirer profit et faire preuve d'une combinaison des compétences diverses en maitrisant à la fois des concepts statistiques avancées, une culture technique variée et une compréhension solide des enjeux métier de son entreprise ou de son administration publique si il est fonctionnaire.

[(1)] voir « *Data scientist: The sexiest job of 21st century* » par Thomas H. Davenport et DJ Patil publié dans Harvard Business Review – Octobre – 2012

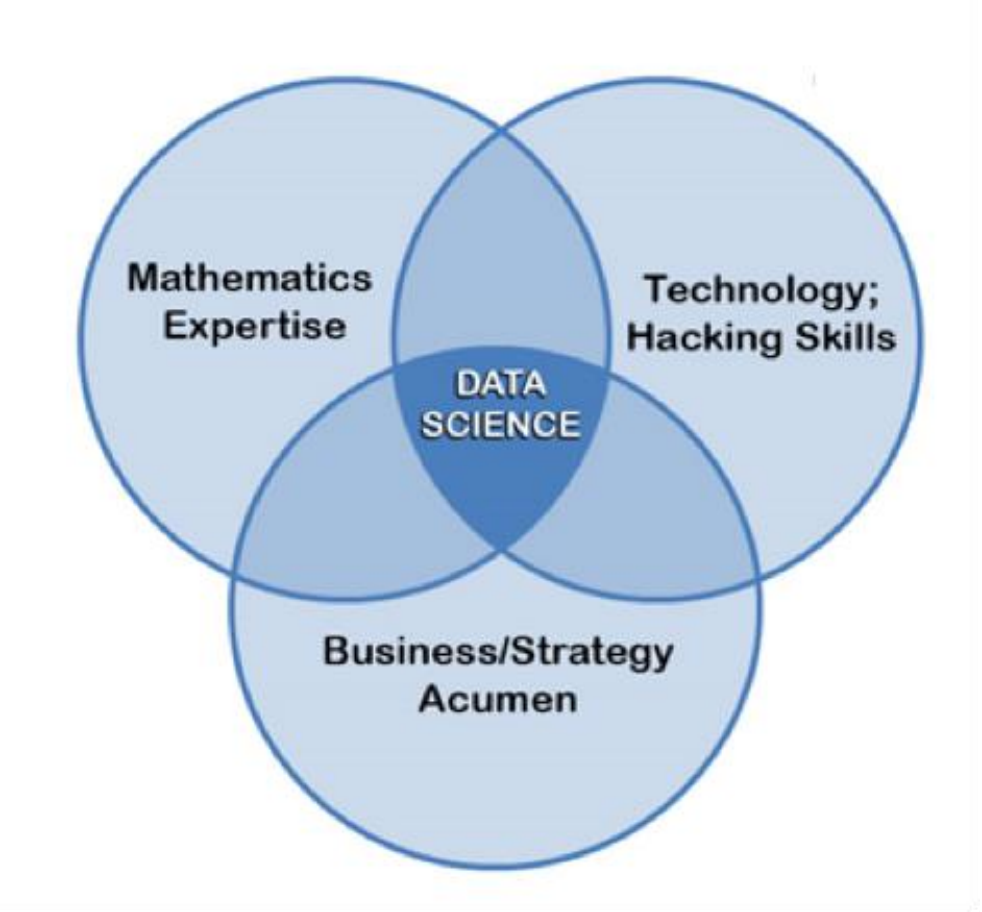


Figure 5 : Schéma illustrant les compétences d'un «data scientist» [(1)]

[(1)] T. DAVENPORT ET D.J. PATIL, « *Data scientist: The sexiest job of 21st century* », Harvard Business Review – Octobre – 2012

Comme l'illustre le schéma précédent, les compétences d'un «*data scientist*» s'organisent autour de trois disciplines principales:

- ***Compétences en mathématiques***:
  Le «*data scientist*» a besoin des connaissances en mathématiques, en statistique, et en algorithme. Ces connaissances lui permettent de comprendre des concepts comme le calcul de probabilités, le niveau de signification, *etc*. La maitrise des algorithmes lui permet de choisir les bons paramètres et les bonnes variables afin d'aboutir au meilleur modèle possible. Le métier de «data scientist» est différent de celui d'un statisticien. En effet, le premier accorde peu d'importance à la pureté statistique d'un modèle qu'à son utilité métier. D'ailleurs, les deux métiers ont un point sur différent sur certaines notions comme le niveau de signification ;

- ***Compétences technologiques***:
  Le «*data scientist*» est amené à utiliser une panoplie de nouveaux outils techniques de Big data comme Hadoop, NoSLQ, Mapreduce, Spark, Hive, *etc*. Son travail au quotidien pour implémenter ses différentes modèles mathématiques nécessite une compréhension des notions informatiques comme le «clustering» pour comprendre les limites techniques des machines ou le «scalling» (passage à l'échelle) pour se familiariser avec les problématiques liées aux grands volumes des données. Le métier de «data scientist» est différent de celui d'un développeur. En effet, le premier accorde peu d'importance à la maitrise parfaite des rouages d'un langage de programmation, il doit seulement être capable de prototyper son modèle pour obtenir le résultat attendu ;

- ***Compétences métier*** :
  Le «*data scientist*» doit comprendre le métier de son entreprise afin d'analyser les enjeux et maitriser sa stratégie. Cette compréhension lui permet de proposer des nouveaux services et produits à base de données analysées.

A partir de ces trois dimensions, le spécialiste américain Thomas Davenport[(1)] liste les différentes compétences nécessaires pour le métier d'un «*data scientist*»:

- *Compétences d'un informaticien*:
  - Capacité à coder ;
  - Compréhension des capacités technologiques du Big data ;

- *Compétences d'un consultant*:
    - Prise de décision sur la base d'indices ;
    - Fortes compétences en communication et en relationnel ;
    - Capacités à encadrer des décisions et à comprendre les procédures associées ;

- *Compétences d'un analyste quantitatif* :
    - Analyse statistique et graphique ;
    - Analyse des données structurées et non structurées ;

- *Compétences d'un expert commercial* :
    - Connaissance du métier ;
    - Capacité à proposer des nouveaux produits à base des données ;

Blaise Heltai, professeur de mathématique et chercheur aux Bell Labs, qui a propulsé ce métier, décrit son travail de «*data scientist* » de la façon suivante:

> *«Nous devions collecter les données à partir des de technologies complexes avant de pouvoir les analyser. Le plus souvent en employant des langages de scripts utilisés aujourd'hui. Les volumes étaient généralement importants – je me souviens avoir analysé les coûts des appels téléphoniques en utilisant les informations transmises par les commutateurs installées dans les centraux, un problème de grande données classiques. Nous avons beaucoup travaillé à la modélisation et l'optimisation, tant sur les aspects financiers que sur le routage des appels. A l'instar de certains projets «big data » actuels, nous avons également cherché à proposer de nouveaux produits. Nous avons évalué la demande et établi des modèles économiques pour de nouveaux services télécoms, mis en place des essaies de terrain ou de nouveaux services, réalisés les premiers tests de smartphones et réussi la première offre de vidéos à la demande. Toutes les composantes de «big data » et de la science des données étaient présentes. Cela m'amère à conclure que les scientifiques des données existent depuis un moment ».*[(2)]

Ainsi, le profil de «*data scientist*» se démarque des profils de développeur, d'analyste ou de statisticien par sa polyvalence et de l'étendue de son champs d'action. Il combine de compétences très variées et est amené à manipuler des outils Big data pour développer des nouveaux produits (des «*data products*») et de nouveaux services.

[(1)] T. DAVENPORT, Big data Strategy, Pearson, 2014, p.92

[(2)] T. DAVENPORT, Big data Strategy, Pearson, 2014, p.92

c) Le rôle de «data scientist» dans le service public

À l'heure où l'utilisation des données numériques apparaît de plus en plus comme le cœur de la révolution numérique, les masses de données produites et détenues par l'État et ses administrations appellent d'autres engagements que la seule ouverture de ces données afin de développer de nombreuses nouvelles utilisations par le Cyber-État.

Pour cette raison et à l'instar des entreprises privées qui créent des fonctions de «*Chief Data Officer* » (CDO), le gouvernement français et marocain doivent en mesure de mettre en place une telle fonction au sein de l'administration publique afin d'appuyer le développement du Cyber-État qui va prendre de plus en plus de place dans le quotidien des citoyens.

C'est dans ce sens que le gouvernement français a choisi de créer cette fonction d'«*Administrateur Général des Données* ». Une fonction placée sous l'autorité du Premier ministre, au sein du Secrétariat général pour la modernisation de l'action publique (SGMAP). Ainsi, le gouvernement français s'inspire de son homologue américain qui constituée une équipe des « *data scientists* » qui viendront entre autres appuyer les programmes de la NSA.

Ainsi, Le rôle du « *data scientist* » dans le secteur public consiste à superviser les grandes analyses de données publiques. Sa mission s'articule principalement autour de trois axes :

- Concevoir et diffuser les politiques et les bonnes pratiques en matière d'analyse des données au sein des administrations publiques ;
- Etablir des partenariats public-privé en matière d'exploitation des données et du développement du cyber-secteur public ;
- Aider les administrations publiques à exploiter efficacement leurs données afin d'améliorer leurs performances.
- Aider à développer le métier de «*data Chief Officer*» au sein de Cyber-État.

Ainsi, le « *data scientist* » viendrait appuyer le rôle d'administrateur des données dans e secteur public afin de mettre en place les piliers fondamentaux pour un Cyber-État qui se configure autour du traitement de la donnée.

C. Les outils techniques de Big data

a) Machine Learning

i. Définition du Machine Learning

Depuis l'antiquité, prédire l'avenir est l'un des rêves de l'humanité : Connaitre le comportement d'un ennemi, prédire l'avenue de la pluie, etc. Ces pratiques divinatoires ont laissé place aujourd'hui à la science, aux mathématiques, aux statistiques et à l'informatique.

L'analyse prédictive appliquée aux politiques publiques est sans doute une avancée considérable dans la gestion de l'État moderne. Il s'agit d'anticiper certains comportements des citoyens et des institutions publiques afin d'obtenir des avantages pour améliorer la gestion et la performance d'un État et de ses administrations. Ainsi, l'analyse prédictive permettrait un État par exemple de :

- Détecter des comportements frauduleux lorsque l'on bénéficie des aides sociales ;
- Estimer le taux de transformation d'un secteur d'activité en particulier ;
- Prédire les risques d'engagement sur un chantier de transformation gigantesque ;
- Anticiper les intentions de vote de citoyens ;
- Découvrir l'orientation des jeunes et offrir des parcours de formation adaptés.

Ces préoccupations des pouvoirs publics ne sont pas nouvelles, elles sont même le pain quotidien des administrations publiques.

L'évolution de l'analyse prédictive est liée principalement au développement des algorithmes prédictifs dont beaucoup ont été développés depuis des décennies. Cette évolution a été appuyée par l'arrivée des nouvelles opportunités technologiques comme les Big data. L'analyse des données produites par l'ensemble des acteurs (administrations, entreprises, citoyens, *etc*.) combinés aux différents outils techniques rend l'analyse prédictive un domaine encore à inventer et à développer par la recherche scientifique.

Le Machine Learning (ML) (ou l'apprentissage automatique en français) est un domaine de recherche le plus proche de l'intelligence artificielle. Cette discipline concerne le développement, l'analyse et l'implémentation de méthodes automatisables qui permettent à une machine (plusieurs serveurs informatiques dans le domaine du Big data) d'évoluer grâce à un processus d'apprentissage, et ainsi de remplir des tâches qu'il est difficile ou impossible d'effectuer à travers des moyens algorithmiques plus classiques.

C'est donc un ensemble d'outils statistiques, géométriques, algorithmes et informatiques qui permettent d'automatiser la construction d'une fonction de prédiction à partir d'un ensemble d'observation ou de données disponibles.

Pour résumer, le Machine Learning est une discipline hybride qui se situe à cheval entre plusieurs sciences et techniques que sont l'analyse statistiques, l'intelligence artificielle, le business Intelligence, et l'informatique.

ii. Algorithme de la machine Learning

Le choix d'un algorithme se fait sur plusieurs critères. Ainsi, Ted Dunning, le célèbre spécialiste de Machine Learning, énumère selon lui, les caractéristiques principales d'un bon algorithme d'une Machine Learning :

- « *La déployabilité* » :
  Un algorithme bien élaboré doit être capable d'être déployer sur des Framework de distribution comme Hadoop ;

- *La robustesse* :
  Un algorithme doit traiter des données structurées comme les données non structurées, incomplètes et incohérente. Un tel algorithme doit privilégier une forme de rusticité ;

- *La transparence* :
  Un bon algorithme doit détecter lui-même la dégradation de ses propres performances au fur et à mesure son processus d'apprentissage évolue ;

- *Adéquations aux compétences disponibles* :
  Un bon algorithme doit être facile à implémenter et ne nécessite pas des compétences rares ou une expertise trop poussée ;

- *La proportionnalité* :
  Le temps consacré au développement d'un bon algorithme doit être proportionnel par rapport aux résultats attendus.

iii. Exemples d'applications du « Machine Learning »

Pour illustrer le rendu d'un tel mécanisme, nous présentons ici quelques exemples d'utilisations concrètes du « Machine Learning » :

- *Les spams de nos boîtes mails* :
  Lorsque nous déplaçons un mail dans les spams, la boîte mail retient en mémoire les caractéristiques de ce mail. Grâce aux algorithmes de «Machine Learning», lorsqu'un mail présentant des caractéristiques similaires nous parviendra à nouveau, notre boîte mail le mettra directement dans nos spams. La boîte mail fait office de garde du corps personnalisé face aux mails que nous jugeons inopportuns ;

- *Le site de vente en ligne d'Amazon :*
  le site de vente est un exemple intéressant d'application du «Machine Learning» dans l'e-commerce. Supposons par exemple que nous effectuons la recherche d'un produit sur Amazon aujourd'hui. Lorsque nous revenons un autre jour sur le site, il est capable de nous proposer des produits en rapport avec nos besoins spécifiques. Et ceci grâce à des algorithmes de «Machine Learning» qui prévoient l'évolution de nos besoins à partir de nos précédentes visites sur le site ;

- *Expérimentations d'IBM*:
  IBM a réussi à extraire à partir des notes prises par des médecins pendant les consultations (notes électroniques), des critères pour diagnostiquer l'insuffisance cardiaque. Ils ont développé un algorithme de «*Machine Learning*» qui synthétise le texte en utilisant une technique appelée» ou « *Natural Language Processing* » (NLP). De la même manière qu'un cardiologue peut lire les notes d'un autre médecin et déterminer si un patient a une insuffisance cardiaque, les ordinateurs peuvent maintenant faire la même chose ;

- *La startup Healint :*
  Healint une start-up à Singapour, a lancé sur Android l'application mobile Migraine Buddy. Cette application permet aux patients migraineux d'identifier les facteurs déclencheurs des migraines et les différents symptômes. L'application utilise des algorithmes de «Machine Learning» qui permettent de mettre en évidence des corrélations entre habitudes de vie et migraines. Le système permet également de comparer l'efficacité des différents moyens pour soulager les douleurs. Les rapports dynamiques que l'application génère permettent d'évaluer au fil des mois le contrôle que nous exerçons sur les migraines, et de transmettre aux médecins des données permettant de l'aider à ajuster son traitement.

Le «Machine Learning» consiste donc à apprendre, en tirant des prévisions de fonctionnement ou de comportement à partir des données existantes.

b) L'outil Hadoop

Hadoop est un framework[1] Open Source conçu pour réaliser des traitements sur des volumes de données massifs Big data . Il est géré sous l'égide de la fondation Apache, et est écrit en langage de programmation informatique Java.

Hadoop a été conçu par Doug Cutting, développeur informatique au sein de la fondation Apache. En 2004, Google a publié un article de présentation de son algorithme MapReduce basé sur des opérations analytiques à grande échelle, Doug Cutting [2] s'en est inspiré pour développer le framework Hadoop.

Hadoop a été conçu pour stocker de très gros volumes de données sur un grand nombre de machines équipées de disques durs. Il permet l'abstraction de l'architecture physique de stockage afin de manipuler un système de stockage distribué (autrement dit système de fichiers) comme s'il s'agissait d'un disque dur unique. Une architecture de machines HDFS (aussi appelée cluster HDFS (Hadoop Distributed File System) repose sur deux types de composants majeurs :

1- *NameNode* (nœud de noms) :
ce composant gère l'espace de noms, l'arborescence du système de fichiers et les métadonnées des fichiers et des répertoires. Il centralise
la localisation des blocs de données répartis dans le cluster. Il est unique mais dispose d'une instance secondaire qui gère l'historique des modifications dans le système de fichiers (rôle de backup). Ce NameNode secondaire permet la continuité du fonctionnement du cluster Hadoop en cas de panne du NameNode d'origine ;

2- DataNode (nœud de données) :
ce composant stocke et restitue les blocs de données. Lors du processus de lecture d'un fichier, le NameNode est interrogé pour localiser l'ensemble des blocs de données. Pour chacun d'entre-eux, le NameNode renvoie l'adresse du DataNode le plus accessible, c'est-à-dire le DataNode qui dispose de la plus grande bande passante. Les DataNodes communiquent de manière périodique au NameNode la liste des blocs de données qu'ils hébergent. Si certains de ces blocs ne sont pas assez répliqués dans le cluster, l'écriture de ces blocs s'effectue en cascade par copie sur d'autres.

---

[1] Un ensemble cohérent de composants informatique.

[2] Voir l'article « Hadoop Daddy Doug Cutting says there's an elephant in the room », The Register, 8 mai 2014.

Le HDFS n'est pas entièrement conforme aux spécifications POSIX[(1)]. Les exigences relatives à un système de fichiers POSIX diffèrent des objectifs cibles pour une application Hadoop. Le compromis de ne pas avoir un système de fichiers totalement compatible POSIX permet d'accroître les performances du débit de données.

Plusieurs grands noms de l'informatique ont déclaré utiliser Hadoop. La fondation Apache a mis disposition la liste des entreprises utilisant Hadoop, on y trouve toutes les grandes entreprises de l'informatique comme Amazon, Microsoft, Google, ou facebook. Ce dernier a déclaré avoir détenir la plus grande architecture Hadoop.

c) MapReduce

MapReduce est un modèle de référence (ou *pattern* en anglais) d'architecture de développement informatique, développé par Google, dans lequel sont effectués des calculs parallèles, et souvent distribués sur plusieurs machines, avec un traitement de données volumineuses [(2)].

MapReduce permet de manipuler de grandes quantités de données en les distribuant dans un cluster de machines pour être traitées. Ce modèle connaît un vif succès auprès de sociétés possédant d'importants centres de traitement de données telles qu'Amazon.com ou Facebook. Il commence aussi à être utilisé au sein des architectures Cloud Computing.

De nombreux frameworks ont vu le jour afin d'implémenter le MapReduce. Le plus connu est Hadoop qui a été développé par Apache Software Foundation. Mais ce framework possède des inconvénients qui réduisent considérablement ses performances notamment en milieu hétérogène. Des frameworks permettant d'améliorer les performances de Hadoop ou les performances globales du MapReduce, tant en termes de vitesse de traitement qu'en consommation électrique, commencent à voir le jour.

---

(1) Une famille de normes techniques définie depuis 1988 par l'Institute of Electrical and Electronics Engineers (IEEE), et formellement désignée par IEEE 1003.

(2) Définition qui en donne wikipédia : http://fr.wikipedia.org/wiki/MapReduce

D. Plan industriel Big data

d) Contexte

Comme nous l'avons vu dans la partie Cloud Computing, la nouvelle France industrielle est le nom donné aux plans de ré-industrialisation de la France mis en place par le gouvernement français et présentés le 12 septembre 2013 par le président François Hollande et Arnaud Montebourg, ministre du Redressement productif (2012-2014).

A travers ce plan stratégique, le gouvernement français a défini 34 plans industriels dont le Big data. Ainsi, sur la base de différents enjeux présentés précédemment autour du Big data, la feuille de route présentée concernant ce plan s'articule autour d'actions spécifiques visant à lever des verrous ou à développer le marché autour de cette technologie via une politique volontariste axée autour de plusieurs des mesures dont nous présentons les principales ci-dessous.

e) La formation des citoyens du Cyber-État

La feuille de route du plan Big data préconise que le système éducatif forme suffisamment de « data scientists », profil au cœur de cette technologie. Les formations devront être à la fois des formations courtes, de type formation continue ou professionnalisante.
En effet, le consensus aujourd'hui est de définir le « data scientist » à l'intersection de trois domaines d'expertise:

- *Mathématiques*: il lui faut de solides connaissances en mathématiques, en statistiques et en algorithmes, pour lui permettre de comprendre des concepts comme le calcul de probabilités, le niveau de signification, etc ;

- *Technologique*: il est amené à utiliser une panoplie de nouveaux outils techniques liés au Big Data, comme Hadoop, NoSLQ, Mapreduce, Spark, Hive… Son travail au quotidien nécessite aussi d'avoir des notions informatiques, en matière, par exemple, de «*clustering*» ou de «*scalling*» ;

- *Métier* : il est essentiel qu'il comprenne parfaitement l'activité, le métier de son entreprise afin de pouvoir maîtriser la stratégie, de savoir identifier les enjeux essentiels… Ce qui lui permettra notamment de proposer de nouveaux services et produits à partir de l'analyse de la base de données.

Ainsi mettre en place un système éducatif qui permet la formation des étudiants aux nouvelles exigences de l'emploi mais également de les sensibiliser aux enjeux de la transformation numérique. Ainsi, la formation des profils de type « *data scientist* » permet aux entreprises privées françaises mais également à l'administration publique françaises d'avoir des compétences formées qui permettent de s'intégrer dans une économie qui certainement serait une économie de la donnée dans les années à venir.

f) Développer un écosystème des start-ups autour du Cyber-État

Une des mesures phares préconisée par le plan de la France industrielle Big Data est de favoriser l'innovation ouverte autour des données et précisément des données publiques. Ainsi, la feuille de route insiste sur la mise en place d'une stratégie nationale pour promouvoir le développement des startups dans le domaine du Big Data via la mise en place d'un « Centre de Ressources Technologiques » fournissant :

- Recensement des données sur lesquelles les grands donneurs d'ordre sont prêts à travailler dans une logique d'innovation ouverte (grands groupe, services de l'État, startups), et garantie de la neutralité dans l'accès à ces données (sans que ce ne soit nécessairement des données « ouvertes ») ;
- Consolidation des initiatives privées de plateforme de collecte de données ;
- Accès à des compétences et des logiciels spécialisés dans le domaine du Big data ;
- Accès à des ressources de calcul à grande échelle pour mener des expérimentations réalistes et construire rapidement des prototypes opérationnels.

En plus, la feuille de route de Big data présente également un certain nombre des mesures sectorielles que nous pouvons résumer dans les points suivants :

- *Projets sectoriels dans le secteur privé* : Identifier les secteurs industriels les plus à risque dans le domaine concurrentiel (Assurance, Energie, Transport) et permettre à ces acteurs privés de mener à bien des expérimentations sur de nouveaux usages de la donnée leur permettant de mener une politique industrielle offensive sur le plan international dans le domaine ;

- *Projets sectoriels dans le secteur public* : Faire de l'Etat un exemple dans le domaine du Big Data, en lançant de grands projets dans les domaines de la Santé et de l'Emploi. Ces grands projets doivent être l'occasion de faire rentrer dans une logique d'innovation ouverte les services de l'Etat concernés ainsi permettre le développement de Cyber-État et les cyber-services publics associés.

Le plan de la nouvelle France industrielle en matière de Big data insiste également sur l'évolution des mesures réglementaires et législatives pour faire évoluer la mise en œuvre de la Loi Informatique et Libertés et la CNIL vers une logique de «certification de processus » et de « label éthique» permettant aux industriels qui y auront recours de promouvoir un approche éthique de l'utilisation des données personnelles et d'en faire un atout concurrentiel, notamment à l'exportation.

Le schéma suivant récapitule les différents mesures phares du plan Big data:

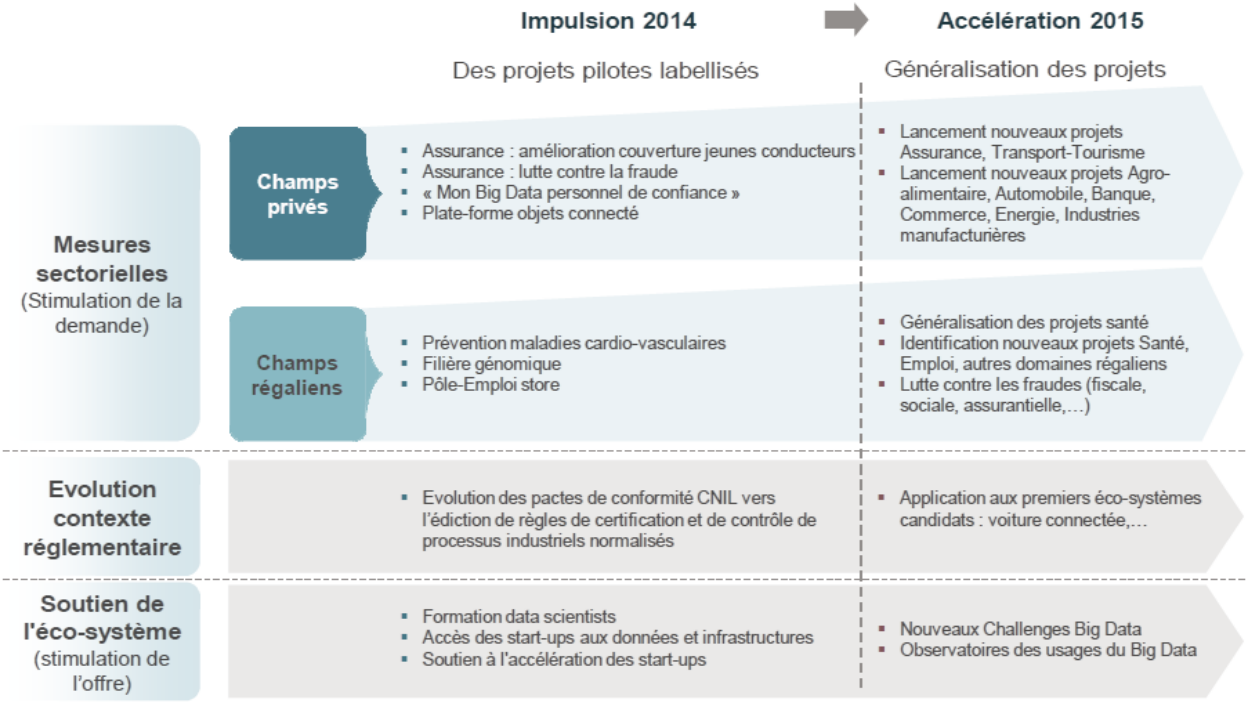


Figure 8 : Schéma des principales mesures du plan Big data[(1)]

---

(1) Schéma issu du Plan France Industrielle disponible sur le lien suivant : http://www.economie.gouv.fr/files/files/PDF/nouvelle-france-industrielle-sept-2014.pdf (dernière consultation 04/09/2016 à 01h10)

E. Mission Etalab et ouverture des données publiques

Comme on peut le lire dans l'article 1 de la loi[(1)] du 1978 relative au droit d'accès aux documents administratifs.

> **[Article 1]**
> « *(…) quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par, l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions et décisions. (…)* ».

Ainsi, le droit d'accès aux documents administratifs a été reconnu comme une « liberté publique » par le Conseil d'État[(2)] depuis 2002. Après en 1997, le gouvernement en a élargi le principe en décidant la mise en ligne gratuite des « données publiques essentielles ». En 2003, la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, transposée par l'ordonnance du 6 juin 2005 et le décret du 30 décembre 2005, a facilité la réutilisation des documents existants détenus par des organismes du secteur public.

Le décret n° 2011-577 du 26 mai 2011 relatif à la réutilisation des informations publiques détenues par l'État et ses établissements publics administratifs a posé le principe de la gratuité du droit à réutilisation.

C'est dans ce contexte que le 21 février 2011, le décret n° 2011-194 portant création d'une mission « Etalab » chargée de la création d'un portail unique interministériel des données publiques créait la structure en charge d'animer et d'héberger la diffusion de ces données publiques.

Ainsi, cette ouverture des données va permettre le développement du Cyber-État principalement à travers l'engagement et le soutien des citoyens et des administrations dans la ré utilisations des données publiques au profit d'une action publique moderne et renouvelée. Ainsi, L'ouverture des données publiques est un outil majeur au service de la transformation du service public, pour en améliorer la qualité et en permettre l'émergence d'un cyber-service public moderne et efficace.

---

(1) voir la loi n° 78-753 du 17 juillet 1978

(2) voir décision conseil d'État : CE, 29 avril 2002, U., n° 228830

Ainsi, selon la feuille de route du Gouvernement en matière d'ouverture et de partage des données publiques, la mission « Etalab » vise principalement les axes suivants :

- Renforcer la confiance des citoyens grâce à une plus grande transparence de l'action publique (par exemple, avec la mise en ligne d'informations sur les comptes publics, la pollution ou les délits constatés) ;

- Améliorer le fonctionnement administratif (comme en témoigne la très forte utilisation des données publiques par l'administration elle-même) ;

- Améliorer l'efficacité de l'action publique en développant de nouveaux modes d'organisation et de nouveaux processus de travail (comme le suivi des accidents de la route par la sécurité routière permettant d'améliorer l'aménagement de la voirie) ;

- Contribuer à l'influence et au rayonnement international de la France à travers des initiatives *comme Open Government Partnership*[(1)].

[(1)] Le Partenariat pour un gouvernement ouvert ("PGO", en anglais: Open Government Partnership ou "OGP") est un accord international sous forme de partenariats entre plusieurs pays visant à promouvoir la transparence dans l'action publique. Les pays fondateurs sont Brésil, Indonésie, Mexique, Norvège, Philippines, Afrique du Sud, Royaume-Uni et États-Unis. Aujourd'hui l'organisation compte 65 pays dont la France et le Maroc. La France présidera l'organisation de septembre 2016 jusqu'au septembre 2017.

4. Chapitre 4 : Autres technologies comme fondement technique du Cyber-État

A. Internet des objets

Définir la notion «Internet des objets » est une tâche difficile impliquant une imbrication de plusieurs notions techniques comme l'informatique, électronique, les réseaux, etc. mais aussi des notions liés à son usage et ses fonctionnalités. Cependant, nous remarquons dernièrement des tentatives pour faire émerger une définition standard qui serait unifiée et utilisée par l'ensemble des acteurs concernés. Cette définition prendrait en compte les aspects techniques de la technologie mais également les aspects liés à son utilisation et ses fonctionnalités. Cette définition aurait pour objectif de vulgariser le concept pour les personnes non-expertes et permettre une adoption plus large et plus rapide au près du grand public.

En regardant la littérature scientifique, nous constatons que l'une des premières définitions de l'Internet des Objets consiste à dire qu'il s'agit d'un ensemble « objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés »[(1)]. Cette définition renvoie sur la capacité à faire connecter des personnes et les objets à travers le réseau Internet. Elle, la définition, met en évidence élimination des contraintes liées à l'espace géographique des objets ou des personnes. En effet, l'opération de connecter des objets, avec d'autres objets ou personnes, à travers le réseau Internet s'appuie sur l'utilisation de plateformes techniques hébergées dans le Cloud Computing (en mode PaaS : Plateforme As A Service) et permettent de connecter plusieurs objets identifiés par des éléments techniques comme une adresse IP, une URL, une puce RFID, etc. Cependant, cette définition de l'Internet des objets est limitée aux aspects techniques de la technologie et n'évoque pas l'aspect usage afin que celle-ci soit une définition complète comme nous l'avons précisé précédemment.

[(1)] Anonyme. 2008. *Internet of Things in 2020. Roadmap for the Future,* 1.1 ed.: 27: Infso D.4 Networked Enterprise & RFID; Infso G.2

Cette définition conjuguant les aspect technique et usage, nous la retrouvons dans une autre tentative qui nous semble complète qui consiste à définir l'Internet des objets comme « *un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant »(2*). Les auteurs de cette définition ont pu identifier les principaux systèmes technologiques nécessaires au fonctionnement de l'Internet des Objets comme le montre ce tableau :

TABLEAU 1 **Principaux systèmes technologiques nécessaires au fonctionnement de l'IdO**

Type de systèmes	Identification (y compris lecteurs)	Capteurs	Connexion	Intégration	Traitement de données	Réseaux
Enjeux	Reconnaître chaque objet de façon unique et recueillir les données stockées au niveau de l'objet.	Recueillir des informations présentes dans l'environnement pour enrichir les fonctionnalités du dispositif.	Connecter les systèmes entre eux.	Intégrer les systèmes pour que les données soient transmises d'une couche à l'autre.	Stocker et analyser les données pour lancer des actions ou pour aider à la prise de décisions.	Transférer les données dans les mondes physiques et virtuels.
Technologies anciennes (exemples)	Codes barres, solutions RFID simples	Thermomètre, hydromètre...	Câbles...	*Middlewares*...	Excel, ERP, CRM...	Internet, Ethernet...
Technologies récentes (exemples)	Solutions RFID complexes, Surface Acoustic Waves, puces optiques, ADN	Capteurs miniaturisés nanotechnologies	Bluetooth, Near Field Communication (NFC), WiFi...	*Middlewares* évolués	Datawarehouse 3D (compatible avec les puces RFID), Web sémantique...	Réseau EPCglobal...

Tableau 1 ; Principaux systèmes technologiques nécessaires au fonctionnement de l'IdO(1)

En lisant ce tableau, il nous semble clairement que l'Internet des Objets n'est pas une seul technologie unique et isolée mais, au contraire, un ensemble des technologies qui nécessitent une interopérabilité technique au niveau des protocoles, standards et normes mais aussi dans l'usage : Pouvoir initier une tache par un objet et être capable de le finir par un autre objet. Cette interopérabilité consiste donc à mettre en place un interfaçage entre les objets utilisant des technologies différentes afin que ces derniers – les objets – puissent se communiquer et comprendre chacun le langage de l'autre.

De ce fait, réduire la communication entre les objets au seul réseau d'Internet n'est pas viable et très réductrice. D'autres réseaux (comme le réseau Zigbee) pourraient devenir un canal de communication au même titre que l'Internet. Cependant, cette multiplication des canaux de communication ne ferait que complexifier encore plus l'interopérabilité et rend l'écosystème d'Internet des objets ingérable et pénaliserait certainement son développement futur.

---

(1) J.P BENGHOZI ET S. BUREAU ET F. MASSIT-FOLLÉA, L'Internet des objets : Quels enjeux pour l'Europe. Paris : Éditions de la Maison des sciences de l'homme, 2009 (nouvelle édition le 20 août 2016)

Le Cyber-Etat, issu de l'État interventionniste dans le domaine numérique, devrait être un acteur principal dans la standardisation de cette technologie, sauf que, sans contrôle démocratique, il peut y avoir des risques sur les libertés dans l'usage pour généraliser une surveillance de masse. Dans le cas de la France par exemple, si nous regardons les techniques autorisées par la loi de 24 Juillet de 2015 sur le renseignement, nous retrouvons les éléments suivants :

- balisage de véhicule ;
- sonorisation de lieux privés ;
- Captation d'images dans des lieux privés, captation de données informatiques ;

Toutes ces opérations pourraient s'automatiser et se réaliser via des objets connectés à travers Internet même si l'Assemblée Nationale a limité l'utilisation des imitateurs d'antennes relais ("IMSI Catcher") qui permettent d'aspirer les conversations dans un périmètre donné.

Pour finir, l'Internet des objets est aujourd'hui et le serait encore demain, un des piliers sur lequel s'appuieraient le fonctionnement du Cyber-État, la représentation de l'État dans la sphère numérique.

B. Intelligence Artificielle

En regardant la littérature scientifique, nous remarquons qu'il n'existe pas une définition unique du concept de l'Intelligence artificielle. D'après nos recherches, la première utilisation du terme « Intelligence Artificielle » est attribuée à Marvin Lee Minsky, chercheur au sein du groupe Intelligence Artificielle du Massachusetts Institute of Technology (MIT) à Boston. Une utilisation qui est apparue dans son article intitulé « *steps toward Artificiel Intelligence* »[(1)]. Ce chercheur, avec John John McCarthy, sont considérés comme les fondateurs de ce concept de l'Intelligence Artificielle.

D'après cette revue de littérature, nous avons pu identifier certaines définitions qui nous semblent pertinentes. Ainsi, l'intelligence Artificielle est considérée donc comme étant :

- « L˝étude des facultés mentales à l'aide des modèles de type calculatoires »[(2)]
- « Conception d'agents intelligents »[(3)]
- « Discipline´étudiant la possibilité de faire exécuter par l'ordinateur des tâches pour lesquelles l'homme est aujourd'hui meilleur que la machine »[(4)]
- « L'automatisation des activités associées au raisonnement humain, telles que la décision, la résolution de problèmes, l'apprentissage,… » [(5)]
- « L'étude des mécanismes permettant à un agent de percevoir, raisonner, et agir »[(6)]
- « L'étude des entités ayant un comportement intelligent »[(7)]

---

(1) Article consultable sur le site de l'université de l'Université de Texas sur le lien suivant : http://www.cs.utexas.edu/~jsinapov/teaching/cs378/readings/W2/Minsky60steps.pdf (consulté le 21/08/2016 à 20h)

(2) E. CHARNIAK ET D. MCDERMOTT, Introduction to artificial intelligence, , Addison-Wesley Publication, 1985

(3) AL. POOL , Minister pretations by Both Sides of the Recovered Memories Controversy, 1998. Définition consultable sur le site de l'Université Of Victoria sur le lien: http://web.uvic.ca/~dslind/sites/default/files/Poole&Lindsay.pdf (consulté le 20/08/2016 à 21h)

(4) E. RICH et K. KNIGHT, Artificial Intelligence, McGraw Hill Inc, 1991

(5) R. BELLMAN, Artificial intelligence, Boyd & Fraser, 1978

(6) P.H WINSTON, Artificial Intelligence, Third Addition: Addison-Wesle, 1992

(7) N. NILSSON, Artificial Intelligence: A New Synthesis, Morgan Kaufmann, 1998.

En analysant ces définitions, nous remarquons qu'elles s'accordent toutes sur le fait qu'une Intelligence Artificielle a pour but de créer des systèmes et des agents intelligents, cependant, elles s'accordent pas pour donner une définition exacte et unifiée du concept de l'intelligence. Cette dernière renvoie chez certain au comportement des systèmes, alors que chez d'autres, elle renvoie vers le raisonnement de ces mêmes systèmes.

Une autre vision nous vient du scientifique Alan Touring qui défend une vision de l'Intelligence Artificielle consistant à créer des systèmes intelligents qui se comporterait comme des être humains. Ainsi, Alan Turing, présentait son célèbre test « Test de Turing » selon lequel une machine est considérée comme intelligente si elle peut converser de telle manière que les interrogateurs (humains) ne peuvent la distinguer d'un être humain. En effet, Alan Touring, dans un article publié en 1950 et intitulé « Computing Machinery and Intelligence », insiste sur le fait que l'Intelligence Artificielle ne se définit pas mais plutôt elle se teste suivant certaines procédures précises. A titre exemple :

- Un individu communique à l'aide d'un terminal d'ordinateur avec un interlocuteur invisible. Il doit décider si l'interlocuteur est un être humain ou un système d'IA imitant un être humain.
- Construire un cerveau artificiel en imitant moins la physiologie du modèle humain, que son comportement logique, les "états de pensée" étant équivalents aux instructions de la machine.
- Il doit y avoir 30 % de réussite pour une machine discutant avec une personne non avertie pendant 5 minutes.

A partir de ces éléments, il nous semble que la technologie de l'Intelligence Artificielle serait également un des piliers du Cyber-État de demain. L'Etat aujourd'hui est fortement concerné par cette technologie et peut l'exploiter principalement dans le domaine de la sécurité et la vidéosurveillance entre autre. Par conséquent, le développement de cette technologie doit s'accompagner par une réclamation associée et stricte de la part de l'Etat afin de faire respecter les droits fondamentaux des citoyens et éviter toute dérive d'utilisation comme en témoigne le cas de la technologie de reconnaissance faciale introduite par facebook et qui a été interdite en France suite à des plaintes portées par la CNIL. Comme l'expliquait la CNIL, « En s'appuyant sur une base de photographies préenregistrées reliée à un système de vidéoprotection et à un dispositif de reconnaissance automatique des visages, il est désormais techniquement possible d'identifier un individu dans une foule. Si cette technologie n'en est qu'à ses balbutiements, il importe de comprendre que son caractère intrusif est croissant puisque la liberté d'aller et venir anonymement pourrait être remise en cause ».

Cette technologie de reconnaissance faciale, qui s'appuie sur la technologie de l'Intelligence Artificielle, est encore utilisée dans d'autres pays et représente une technologie qui serait très bénéfique pour les services du Cyber-État. Reste à cadrer et à contrôler l'utilisation d'une telle technologie.

Conclusion

IV. Conclusion

L'idée de départ de notre recherche consiste en l'analyse des politiques publiques françaises et marocaines en matière d'adoption et du développement des technologies de Cloud Computing et de Big data. En effet, nous avons souhaité analyser ce que les deux États – français et marocain – font (ou ne font pas) pour faire face aux nouveaux enjeux provoqués par le numérique et précisément par les deux technologies en question. Ainsi, à travers ce travail, nous avons principalement couvert quatre axes principaux de recherche que nous résumerons dans les quatre parties qui suivent.

1) De l'État au Cyber-État

Le premier axe consiste à analyser l'évolution de l'État, depuis sa conception classique wébérienne, vers un Cyber-État. En effet, nous pensons que les enjeux à la fois politiques, économiques et sociaux autour de Cloud Computing et de Big data constituent une nouvelle problématique à laquelle l'État d'aujourd'hui doit apporter une réponse politique mais également technique. Ainsi, l'État, selon les conceptions classiques, se voit transformé avec une nouvelle représentation de ses missions dans le cyberespace à travers le Cyber-État. Ainsi, un État souverain, selon la conception wébérienne, repose sur quatre éléments fondamentaux qui sont : L'espace géographiquement délimité, le caractère institutionnel induisant un rapport d'autorité à obéissance et un monopole de la légitimité de la violence.

Ainsi, nous remarquons que le Cloud Computing et le Big data ont permis, comme fondements techniques, l'émergence du Cyber-État selon les principes suivants :

- Remise en cause de l'aspect territorial délimité d'un État : En effet, les applications mises à disposition dans le Cloud pour les utilisateurs peuvent être assimilées à un territoire donné. Les utilisateurs de ces applications sont considérés, à leurs tours, comme des citoyens apparentant à ce territoire virtuel, donc des cyber-citoyens. Ainsi, ils s'y forment une population. De ce fait, les utilisateurs de ces applications, ces cyber-citoyens de toutes nationalités confondues, pratiquent les tâches de la vie quotidienne dans ce cyberspace sans aucune restriction géographique. Ainsi, considérer un État comme un espace géographique délimité est totalement remis en question.
- Remise en cause de l'aspect obéissance à l'autorité de l'État : En effet, les plateformes Cloud Computing sont soumises au droit et aux règles juridiques de l'État qui les hébergent et non à celui où se trouvent les utilisateurs, ou les cyber-citoyens, qui s'y connectent. Ainsi, les différences des règles juridiques selon le pays d'hébergement de chaque plateforme, les différentes Conditions Générales d'Utilisation (CGU) de chaque plateforme Cloud ne font que transformer les rapports du pouvoir entre les différents acteurs impliqués : État, l'utilisateur et la plateforme Cloud. Ainsi, ce rapport d'autorité «Plateforme Cloud – Utilisateur» vient remplacer

le rapport classique « État – Citoyen » en donnant naissance à un nouveau rapport « Cyber-État – cyber-Citoyen » au sein du Cyber-État.

- Remise en cause de l'aspect du monopole de légitimité de la violence : En effet, les plateformes Cloud Computing ont un pouvoir de coercition et peuvent ainsi jouer le rôle assimilé à celui d'une police dans le monde réel. Ainsi, elles jouent un rôle dans le contrôle des contenus diffusés aux utilisateurs, ils contrôlent l'accès à Internet, à l'information et au savoir tout en mettant en place des mécanismes pour favoriser un certain type de contenu à l'aide des technologies de Big data. Elles ont également la capacité à traiter les données personnelles des utilisateurs, à surveiller le comportement des utilisateurs, à les contrôler et à les bannir si ces utilisateurs ne respectent pas les conditions générales d'utilisation (CGU). Nous pouvons donc assimiler ces activités aux activités classiques des services de renseignement d'un État.

Ainsi, nous considérons que le Cyber-État est une continuité logique de la notion classique de l'État dans le cyberspace. Cette continuité de l'État dans le monde virtuel implique:

- Le développement d'un « cyber-secteur public » au sein du Cyber-État comme une extension de l'ensemble des représentations centrales ou locales de l'État dans le cyberspace. Ainsi, le Cyber-État assure sa domination et son contrôle et oriente le fonctionnement de toutes ces plateformes qui constituent l'extension du secteur public sur Internet ;
- L'extension du « cyber-service public » au sein de du Cyber-État. En effet, si nous considérons les trois principes de service public (continuité, égalité et mutabilité) d'un prisme numérique, on constate que les outils numériques et précisément la disponibilité des services en mode Cloud Computing permettent d'assurer une continuité de services publics, une égalité d'accès à tous les utilisateurs et une évolution des règles et d'adaptation aux nouvelles exigences légales. Ainsi, plusieurs démarches administratives pourront être accomplies seulement via Internet. Ainsi, dans l'avenir, plusieurs services publics pourront être automatisés et industrialisés et mis à disposition sur Internet. Ils représenteront une continuité du service public dans le cyberspace.
- Elaboration et adoption des « cyber-politiques publiques ». En effet, les « cyber-politiques publiques » correspondent aux programmes d'action qu'une autorité publique met en place pour un secteur d'activité particulier au sein du Cyber-État afin de résoudre des problèmes publics et répondre à des attentes des cyber-citoyens. Ainsi, ces « cyber-politiques » constituent une prolongation logique des politiques publiques classiques. Leurs études, pour reprendre les termes de Thomas Dye, reviennent à l'étude de l'État en action.

2) Cybersécurité à l'ère du Cyber-État

Face aux risques de tensions sociales et politiques provoqués essentiellement par le numérique, la France, comme le Maroc, se sont dotés des instruments juridiques et techniques qui s'appuient principalement sur les technologies de Cloud Computing et de Big data. Ainsi, l'arsenal juridique français s'est vu renforcé par l'adoption successive et accéléré, sans débat national consultatif, des lois visant à restreindre les libertés publiques pour, entre autres, lutter contre le terrorisme et assurer la « sécurité nationale ». Ces textes sont:

- La loi de programmation militaire 2014-2019 (PLM) adoptée en 2013, en continuité avec celle de 2008, qui souligne dans article L. 241-2 le droit d'intercepter toutes les communications électronique dans le cadre d'une atteinte à la « sécurité nationale ». déjà inscrite dans la loi de 1991 sur les interceptions des communications électronique pour des besoins de sécurité nationale. Ainsi, l'adoption de cette loi et précisément son article 20 manifeste une profonde crise d'un pouvoir politique n'hésitant plus à porter massivement atteinte aux droits fondamentaux sous prétexte des impératifs de la défense et de lutte contre le terrorisme ;
- La loi anti-terrorisme adoptée en 2014 consiste à renforcer la lutte contre le terrorisme et à prendre en compte les évolutions récentes des actes de terrorisme et spécialement ses aspects technologiques. Le texte renforce la répression de l'apologie du terrorisme et de la provocation à des actes pouvant atteindre la sécurité nationale. Cependant, si la lutte contre le terrorisme est légitime surtout dans un contexte internationale tendu elle ne peut pas justifier de légiférer en urgence sans lancer des débats nationaux qui vont permettre à l'ensemble de la population : citoyen, experts, décideurs politiques, etc., de s'exprimer et éviter mettre en place des lois avec des graves atteintes aux libertés fondamentales ;
- La loi relative au renseignement, adoptée après les attentats de Janvier 2015, en discussion depuis deux ans, validée définitivement le 24 juillet 2015 et entrée en vigueur le 03 Octobre 2015, vise à donner un cadre légal pour les activités des services de renseignement, qui fonctionnent jusqu'à présent dans un cadre illégale, pour faire face à toute atteinte à la sécurité nationale . Les finalités de cette loi sont légitimes mais cette constitue une atteinte au respect des droits fondamentaux des citoyens sous prétexte de la sécurité nationale et représente un certain nombre de points inquiétants qui nécessitent un débat élargi. D'autant plus que le contenu juridique de cette notion de sécurité nationale n'a jamais été clairement défini[(1)].

[(1)] G. PERIES, La confiance au prisme de la « sécurité nationale». Une analyse critique à l'ère des réseaux numériques, Politiques sécuritaire et surveillance numérique, P-A CHARDEL (Coord), Paris, Hermès, 2014, P.59.

Ces différents textes ont agité le débat politique français qui a connu une inquiétude grandissante de déploiement de dispositifs numériques de surveillance. Une surveillance, ou une cybersurveillance au sein du Cyber-État, qui se légitime par la lutte contre le terrorisme en faisant, chaque fois que nécessaire, référence à la notion de la sécurité nationale considérée comme restrictive des libertés publiques et individuelles. Son contenu n'est pas défini et est donc flou et reste à la discrétion des autorités publiques.

3) Vie numérique du cyber-citoyen

Dans un contexte de transformation profonde de la société induite par le numérique, l'État doit ré affirmer son droit sur son territoire afin de sécuriser la vie numérique de ses cyber-citoyens. Aujourd'hui, Internet en s'appuyant sur le Cloud Computing et le Big data offre aux individus ; ou aux cyber-citoyens ; des possibilités de sociabilité croissante à travers une vie numérique constituant, dans le Cyber-État, le prolongement de la vie réelle. Cette vie numérique des individus évolue en parallèle à l'évolution de la technologie et des dispositifs sociotechniques qui représentent les innovations poussant la sociabilité en ligne. Cette sociabilité s'accompagne des contraintes liées au traitement des données personnelles et fait surgir des débats sur la vie privée et la sphère privée ainsi que l'émergence du terme « *privacy* » qui peut avoir plusieurs signification comme le droit à la vie privée (*Right Of Privacy*) où à la protection de la vie privée (*Privacy Protection*).

La notion de protection des données personnelles consiste en l'ensemble des mesures visant à assurer le respect du droit. Le Cyber-État doit jouer le rôle du garant du respect des normes et textes juridiques et réglementaire et veiller à ce que cela ne se chevauchent avec les textes de lois cités précédemment et ayant objectifs de réduire les libertés publiques pour des raisons de sécurité nationale. Cependant, l'étude des textes juridiques et réglementaires fait ressortir six thèmes principaux, suivant lesquels s'alignent les diverses réglementations. Ces thèmes sont :

- L'information de l'utilisateur ;
- Le consentement de l'utilisateur ;
- Le droit d'accès et de modification pour l'utilisateur;
- Le principe de justification de la collecte et du traitement ;
- La conservation des données et leur transmission à des tiers.

Ainsi, les institutions comme la Commission Nationale des Libertés et Informatique (CNIL) en France et la Commission Nationale de Protection des Données Personnelles (CNDP) au Maroc ont pour mission de veiller au respect des vies privées et au bon traitement des données personnelles des citoyens au niveau nationale mais également régionale (espace de la francophonie avec la G29). Ainsi, ces institutions détiennent un droit de regard sur les pratiques de l'État vis-à-vis le déploiement des outils de surveillance de masse. Cependant la CNIL française a été mise à l'écart lors de la constitution de la loi sur le renseignement. Néanmoins, d'autres organisations comme la « Quadrature du Net » jouent un rôle de

sensibilisation aux dérives qui peuvent prendre l'adoption hâtive, et sans débat ouvert, de textes de lois légitimant la mise en place des outils de surveillance de masse.

4) Le système au service du Cyber-État

La construction du Cyber-État se base principalement sur un système technique. Ce dernier se caractérise principalement par l'articulation de trois éléments principaux:

- Internet : Qui constitue le réseau des réseaux. En effet, Internet fut une invention militaire américaine qui par la suite s'est développé en se séparant du réseau militaire pour devenir un bien commun gérer par des instances mondiales de gouvernance. Ainsi, l'Internet permet ; entre-autres ; de relier les plateformes Cloud Computing ainsi une diffusion de l'information à travers ces dernières.
- Cloud Computing : Qui renvoie vers une consommation de l'informatique sous forme d'un service fourni par un prestataire, public ou privé, dédié. Ainsi, les applications hébergées dans le Cloud Computing font appel aux technologies de Big data afin d'offrir les services aux utilisateurs finaux.
- Big data : Qui renvoie vers le traitement d'une grande masse de donnée. Ces données peuvent être de types et de sources différentes. Ainsi, en s'appuyer sur des algorithmes optimisés et sophistiques, cette technologie permet de prédire des évènements, des comportements mais également de contrôler l'individu à son insu.

Cependant, comme l'Internet est devenu vitale dans nos quotidiens, il est devenu le centre d'enjeux politique à l'échelle internationale. Ainsi, nous assistons à plusieurs formes de débats et de négociations par la gestion de son infrastructure mondiale comme l'adressage des adresses IP, l'attribution des noms des domaines, le développement des protocoles. Principalement, trois courants émergent à partir de ces débats :

- Les États-Unis qui ne semblent pas vouloir réduire son contrôle sur l'ensemble des instances gérants l'architecture d'Internet. Ils revendiquent leurs légitimité de domination à partir des facteurs historiques et du fait qu'ils ont largement contribué au développement des infrastructures et à la mise en place d'une gouvernance de l'Internet telle qu'elle est aujourd'hui.
- Les pays Européens dont la France, qui adoptent une position modérée, proche de celle des États-Unis. Ainsi, ils souhaitent empêcher que les différentes instances de régulation d'Internet ne soient soumises à des régimes « fermés ». Cependant, ils espèrent revoir les dispositifs actuels et réduire la domination américaine avec une implication plus significative de l'Union Européen.
- Les BRICS, l'Iran, l'Arabie Saoudite et d'autres régimes semblables. Ces pays souhaitent placer ces instances de gouvernance sous le contrôle d'Union International des Télécommunications (IUT). En effet, ils désirent impliquer l'ensemble des États dans la définition des grandes orientations pour l'Internet de demain tout en respectant la cybersouveraineté de chaque Cyber-État. Ainsi, les instances actuelles ne seront plus

sous influences américaine mais elles deviendront indépendantes mais soumises au contrôle des Cyber-États ;

Ainsi, ces tensions et cette domination américaine poussent l'ensemble des pays à développer des alternatives nationales qui permettront d'assurer une autonomie numérique. En effet, cette tendance a été accélérée par les révélations des affaires d'espionnage par la NSA poussant vers une balkanisation de l'infrastructure Internet et au développement des solutions techniques nationalistes isolées.

C'est dans ce sens que la France a adopté une stratégie nationale dans le cadre du plan « France Industrielle », lancé en deux phase entre 2012 et 2014 par le ministre de l'économie et des finances, qui va permettre le développement des solutions française autonomes de type Cloud Computing. Les deux projets principaux sont Numergy et Cloudwatt dont l'État est actionnaire à hauteurs de 35% via la Caisse de Dépôt et Consignations. La France a également développé des références de confiance pour les fournisseurs Cloud Computing étrangers souhaitant travailler avec les entreprises et administrations publiques françaises. De son côté, le Maroc, en s'appuyant sur des partenaires technologiques, a mis en place une feuille de route pour développer également une alternative nationale qui permet d'assurer la souveraineté du pays d'un point de vue numérique.

Egalement dans le cadre de la stratégie « France Industrielle », nous constatons une volonté politique de développer des technologies ainsi permettre l'introduction de cette technologie dans les mécanismes du fonctionnement de l'État français comme en témoigne la mise en place d'un « administrateur générale des donnée » ou « Chief Data Officier ». Ce dernier aura comme mission de développer l'exploitation de la donnée pour améliorer le fonctionnement de l'État mais il garde également un rôle consultatif concernant l'utilisation de ces technologies dans le cadre de la mise en place des lois ayant pour objectif la collecte et la surveillance des comportements des citoyens.

Cependant, d'un point de vue comparatif des modèles français et marocain, nous avons observé une convergence des politiques publiques des deux pays vers les mêmes objectifs et essentiellement au niveau de la structure institutionnelle. En effet, nous remarquons une similitude des lois et textes législatifs adoptés pour des besoins de sécurité nationale, qui renvoie vers la même notion mais qui ne fait référence à aucune définition précise dans les deux pays et reste, comme nous l'avons mentionné précédemment, au gré d'interprétation des autorités françaises et marocaines.

Au niveau institutionnel, nous retrouvons les mêmes structures dans les deux pays comme les commissions nationales chargées de la protection des données personnelles, les structures dédiées au développement du numérique, les laboratoires publiques de recherche et développement, etc. A titre d'exemple, les ministères en charge du numérique ont les mêmes responsabilités du développement des politiques publiques autour du

numérique comme le développement des clusters numériques, aides aux entreprises numériques innovantes, etc.

Cependant, les deux États ont évolué vers des politiques publiques caractérisées par une forte sectorisation institutionnelle et par la délégation à des experts non gouvernementaux des activités de réglementation comme en témoigne la délégation à la CNDP et la CNIL la mise en œuvre de la politique publique liée à la protection des données personnelles. En effet, les deux structures Commission Nationale de Données Personnelles (CNDP) et la Commission Nationale des Libertés et Informatique (CNIL) ont plusieurs points en commun. Les deux institutions ont les mêmes statuts, mêmes missions, etc. Cependant, nous remarquons que la commission marocaine a du mal à s'imposer, vu qu'une grande partie du secteur numérique au Maroc reste au stade informel. Ainsi, la commission marocaine travaille essentiellement avec les administrations publiques, les multinationales installées au Maroc et quelques entreprises marocaines structurées.

La même tendance est également remarquée en matière des initiatives liées au Cloud Computing et Big data. En effet, ces initiatives sont mures et bien avancées en France qu'au Maroc qui n'est qu'en phase expérimentation d'adoption de certaines technologies qui se limitent principalement aux phases études. Au même moment, la France a mis en place les bases solides pour développer les deux technologies comme la mise en place des plans Cloud Computing et Big data dans le cadre de la nouvelle France. Ainsi, en France, une nouvelle loi dédiée au numérique est attendue d'ici Décembre 2015. Une loi sensée encadrer les activités numériques en terme de fiscalisation numérique mais également d'encadrement d'impact du numérique sur les autres secteurs d'activités et éviter de reproduire le scénario vécu avec le secteur des taxis. Le Maroc suit la même trace et prépare également son arsenal judiciaire pour prendre en compte l'impact du numérique sur le quotidien des cyber-citoyens.

Vendredi 23/10/2015, 14h30.

Bibliographie

V. Bibliographie

Abbadi Imad et Martin Andrew, Trust in the Cloud: Information Security Technical Report, 2011.

Alecian Serge et Foucher Dominique, Le management dans le service public, Paris, Édition d'organisation, 2002.

Agamben Giorgio, Qu'est-ce qu'un dispositif ?, Rivages, 2014.

Alali Fatima et Chia-Lun Yeh, Cloud Computing: Overview and Risk Analysis, Journal of Information Systems, 2012.

Allard Laurence et Vandenberghe Fréderic, Express yourself ! Les pages perso, réseaux, N° 1, 2003.

Allison Graham et Zelikow Philip, Essence of Decision, New York, Longman, 1999.

Alverstand Harald et Hakon Lie Wium, Development of Core Internet standards: The work of IETF and W3C, In Bygrave, L. et Bing J (Eds), p.126-149, 2009.

Anderson James, Public Policy Making, New York, Praegger , 1975.

Arquilla John et Ronfeldt David., « Cyberwar is coming ! », Comparative Strategy, vol. 12, n°2, p. 141-165, 1993.

Armbrust M Michael Fox Armando, Griffith Rean, Joseph Anthony, Katz Randy, Konwinski Andrew, Lee Gunho, Patterson David, Rabkin Ariel, Stoica Ion, Matei Zaharia, Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.

Baase Sara, A Gift of Fire: Social, Legal, and Ethical Issues in Computing, Prenctice-Hall, 2003.

Bachelard Gaston, La formation de l'esprit scientifique, Librairie J Vrin, 2000.

Banque Mondiale, Rapport sur l'Administration et l'Education au Maroc, octobre 1995.

Bardach Eugene, The Implementation Game. What happens After a Bill Becomes a Law, Cambridge, Massachusetts, MIT Press, 1977.

Barouch Gilles, Chavas Hervé, Où va la modernisation ? Dix années de modernisation de l'administration d'état en France, Harmattan, 1993.

Barilari André, La modernisation de l'administration, LGDJ, 1994.

Bauer Alain, Violences et insécurité urbaines, Presses universitaires de France (Puf), 2006.

Baumgartner Frank, « Political Agenda », Batles , New York, 2001.

Beaud Olivier, La puissance de l'Etat, Paris, PUF, 1994.

Bellman Richard, Artificial intelligence, Boyd & Fraser, 1978

Bégin Marc-Elian, Jones Bob, Casey James, Laure Erwin, Grey François, Loomics Cal, Kubli Rolf, An EGEE comparative study: Grids and Clouds-evolution or revolution. EGEE III project Report, 2008.

Benhamou Bernard, Organiser l'architecture de l'Internet, revue Esprit, Mai 2006.

Ben Achour Yadh., Droit administratif, CERP, Tunis, 1982, p. 24.

Benghozi Pierre-Jean, Bureau Sylvain, Massit-Folléa Françoise, L'Internet des objets : Quels enjeux pour l'Europe. Paris : Éditions de la Maison des sciences de l'homme, 2009 (nouvelle édition le 20 août 2016)

Bergé Frédéric, «Le sommet de Dubaï entérine la fragmentation de l'Internet mondial», Revue 01Net, 17 décembre 2012.

Betz David et Stevens Tim, Cyberspace and the State, Toward a Strategy for Cyberpower, The International Institute for Strategic Studies, Routledge, Londres, 2011.

Bezes Philippes, Réinventer l'Etat. Les reformes de l'administration française (1962-2008), PUF, Paris, 2009.

Bodiguel Jean-Louis, Quermonne Jean-Louis, La haute fonction publique sous la 5eme République, Paris, PUF, 1983.

Bongrand Philippe et Laborier Pascal, revue française des sciences politiques, 2005.

Rolland Louis, Précis de droit administratif, Dalloz, 1938.

Bollier David, The promise and perils of Big Data, The Aspen institute, 2010.

Boltanski Luc et Chiappello Eve, Le nouvel esprit du capitalisme, Gallimard, 1999.

Boudin Jean, Six livres de la République, Fayard, 1986.

Bourdieu Pierre, Les Règles de l'art. Genèse et structure du champ littéraire, Paris, Seuil, coll. «Point-Essais », 1998.

Boussaguet Laurie, Jacot Sophie, Ravinet pauline, dictionnaires des politiques publiques, Lespresses Sciences Po, 2010.

Boumediene Malik, La question de la modernisation de l'Etat dans le monde arabe : L'exemple du Maroc, Pyramides, 2010.

BURDEAU Georges, Problèmes politiques fondamentaux de l'Etat, ed. Les cours de droits, 1968-1969, p. 383.

Boyd Danah et Kate Crawford, Six Provocations for Big Data, presentation au symposium "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society", Oxford Internet Institute, 2011.

Boyer Bertrand, Cyberstratégie : l'art de la guerre numérique, Nuvis, Paris, 2012.

Brynjolfsson Erik and Andrew McAfee, The Big Data Boom is the Innovation Story of Our Time, The Atlantic, 2011.

Buyya Rajkumar, Yeo Chee Shin, Venugopal Srikumar, Broberg James, Brandic Ivona, Cloud Computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 2009.

Cardon Dominique, La démocratie Internet : Promesses et limites, Seuil, 2010.

Carr Jeffrey, Inside Cyber Warfare: Mapping the Cyber Underworld, O'Reilly Media, 2011.

Charniak Eugene et McDermott Drew, Introduction to artificial intelligence, , Addison-Wesley Publication, 1985

Chellappa Chellappa, Cloud Computing: emerging paradigm for computing, In INFORMS, 1997.

Chevalier Jacques, Le service public, coll. « Que sais-je ? », PUF, 2ème édition, 1991

Couffignal Louis, La cybernétique, Presses Universitaires de France (PUF), 1963.

Cobb Roger et Edler Charles, Participation in American Politics: The dynamics of agenda building, Baltimore, John Hopkins University Press, 1983.

Conesa Pierre, La fabrication de l'ennemi ou comment tuer avec la conscience pour soi, Robert Laffont, 2011.

Crépin Ludivine, Vercouter Laurent, Jacquenet François, Demazeau Yves et Boissier Olivier, « Hippocratic multi-agent systems ». The International Conference on Enterprise Information Systems (ICEIS'08). Pages 301–307, 2008.

Chen Xiaoyu, Wills Gary, Gilbert Lester, Bacigalupo David, Using Cloud for research: a technical review, JISC final report, 2010.

Chevalier Jacques et Loschak Danièle, Science administrative, 1978, LGDJ, 1978.

Choi, Hyunyoung et Hal Varian, Predicting the Present with Google Trends, Keynote address at the Australian Conference of Economists, July 2011, Research Paper, 18 décembre 2011.

Crozier Michel, Etat modeste, Etat moderne, Fayard, 1997.

Curien Nicolas et Maxwell Winston, La neutralité d'Internet, La découverte, 2011.

Davenport Thomas et Harris Jeanne, « What People Want (and How to Predict It) », MIT Sloan Management Review, 9 janvier 2009.

Davenport Thomas, «Big data Strategy» , Pearson, 2014, p.92

Davenport Thomas, Leandro Dalle Mule et John Lucker, « Know What Your Customers Want Before They Do », Harvard Business Review, December 2011.

Dahl Robert, Congress and Foreign Policy, New Haven, Yale Institute of International Studies, 1949.

Dan Nguyen Geofroy et Dejean Sylvain, Le numérique : Economie de partage et de transactions, Economica, 2014.

Demchak Chris, Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI), Center for Cyber Conflict Studies, US Naval War College, 2012.

De Nardis Laura, Protocol Politics: The Globalization Of Internet Gouvernance, MIT Press, P. 25-26-27, 2009.

De Malberg Carré, Contribution à la théorie générale de l'État, Tome 1, Librairie de la Société du recueil Sirey, Paris, 1920.

Deleuze Gilles, « Post-scriptum sur les sociétés de contrôle », Pourparlers, Paris, Éd. de Minuit, 1990.

Desforges Alix, Les représentations du cyberespace: un outil géopolitique, La Découverte, Paris, 2014.

Dilthey Wilhelm, Introduction aux sciences de l'esprit, Broché, 1992

Donath Judith, Signals in social supernets, journal of computer - Midiated Communication, 2007

Duguit Léon, Traité constitutionnel tome III, 3° édition , 1927 , p. 61.

Duguit Léon, Des fonctions de l'Etat moderne, Rev. intern. de sociologie, 1894.

Duff Robert et Papillon Jean-Claude, Gestion publique, Paris, Vuibert, 1988

Duran Patrice, Penser l'action publique, Paris, LGDJ, coll. « Droit et Société », série «Politique», 1999.

Dunn William, Public Policy Analysis: An Introduction, EnglandWood Cliffs, Prentice-Hall, 1981.

Dunn-Cavelty Myriem, Cyber-Security and Threat Politics. US Efforts to Secure the Information Age, Routledge, Abingdon, 2008.

Dunsire Andrew, Implementation in a Bureaucracy: the Execution Process Oxford, Martin Robertson, 1978.

Dupuy François et Thoenig Jean-Claude, L'administration en miettes Paris, Fayard, 1985

Durkheim Emile, Le socialisme. Sa définition – Ses débuts – La doctrine Saint-Simonienne, Paris: Les Presses universitaires de France. 1928.

Duval Claude et Ettori François, « États fragiles… ou états autres ? Comment repenser l'aide à leur développement, notamment en Afrique ? » , Géostratégiques n° 25, octobre 2009.

Dye Thomas, Understanding Public Policy , Englewood Cliffs N.J, PrenticeHall, 1972.

Easton David, A framework for political Analysis, Englwood Cliffts, Prentice-Hall, 1965.

Economides Nicholas et Tag Joacim, Net Neutrality on the Internet: A Two-sided Market Analysis, New York University, 2007

EDWARDS Paul, The Closed World. Cambridge, MIT Press, 1996.

Eggert Lars, From Research to Internet Standards, 30th Brazilian Symposium On Computer Networks and Distributed Systems. Ouro Preto, Bazil , 2012.

Eisenhardt Kathleen et Graebner Melissa, Theory Building From Cases: opportunities and challenges, Academy of Management Journal, 2007.

El Yacoubi Mohamed, « La déconcentration administrative à la lumière du décret du 20 octobre 1993 », REMALD, n°6, 1996.

Etro Federico, The Economics of Cloud Computing. IUP Journal of Managerial Economics, 2011.

Etude du cabinet McKinsey, « Accélérer la mutation numérique des entreprises :un gisement de croissance et de compétitivité pour la France» , Novembre 2014.

Etude du cabinet Roland Berger, Du rattrapage à la transformation: L'aventure numérique, une chance pour la France, Septembre 2014.

Espada Javier, Molina Arturo, Jiménez Guillermo, Concha David, Tenant-based resource allocation model for scaling Software-as-a- Service applications over cloud computing infrastructures. Future Generation Computer Systems, 2011.

Favereau Olivier, Règles, Organisation et Apprentissage collectif : Un paradigme non-standard pour trois théories hétérodoxes, 1992.

Fayon David, Géopolitique de l'Internet, Paris, Economica, 2013.

Ferlie Erwan, The New Public Management in Action, Oxford University Press, 1996.

Flichy Patrice, Le sacre de l'amateur Sociologie des passions ordinaires à l'ère numérique, Seuil, 2010.

Foucault Michel, L'Ordre du discours, Paris, Gallimard, 1971.

Foucault Michel, Surveiller et punir, Naissance de la prison, Paris, Gallimard, 1975.

Garraud Philippe, «Politiques nationales, élaboration de l'agenda», L'année sociologique, 1990.

Gavard-Perret Avenier, Méthodologie de la recherche en sciences de gestion : Réussir son mémoire ou sa thèse, Paris, Pearson, 2012.

Genieys W, Sociologie politique des élites, Paris, Armand Colin 2011.

Gensollen Michel, Les communautés en ligne : échanges de fichiers, partage d'expériences et participation visuelle, Editions Esprit, 2006.

Giddens Anthony, La Constitution de la société, Paris, PUF, 1987.

Giordano. Yvonne, Conduire un projet de recherche. Une perspective qualitative, EMS, 2003.

Giroux Nicolas, «L'étude de cas », in GIORDANO Y. (Coord.), Conduire un projet de recherche: une perspective qualitative, Paris, EMS Management & Société, 2003.

Galdemar Virginie, Gilles Léopard, Simon Marie-Odile, Performance, efficacité, efficience : les critères d'évaluation des Politiques sociales sont-ils Pertinents ?, CREDOC, Paris, 2012.

Glasser Barney et Strauss Anselm, The Discovery of Grounded Theory: Strategies for Qualitative Research, Aldine Transaction, 1967.

Gille Bertrand, Histoires des techniques, Gallimard, Paris, 1978.

Grossman Lev , « How Computers Know What We Want – Before We do », Time Magazine, 27 mai 2010.

Goggin Malcom, Lester James, O'Toole Laurence, Bowman Ann, Implementation Theory and practice: a third generation, scott Foresman and Co, 1990.

Granger Marc-Antoine, Constitution et sécurité intérieure. Essais de modélisation juridique, Paris, LGDJ, 2011.

Granjon Fabien, Reconnaissance et usages d'internet, Les Presses des Mines, 2012.

Granjon Fabien, Denouël Julie, « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », Sociologie 2010/1 (Vol. 1), p. 25-43.

GRENIER Corinne et JOSSERAND Emmanuel, Recherches sur le contenu et recherches sur le processus, dans Méthodes de recherches en management, Paris, Dunod, 2003.

Guerre Talon, « Une frontière public/privé : pour quoi faire ? », Document de recherche CERAM, n°61, 1995.

Gupta Rajen et Ruohonen Miko, Deodhar Sawanand, Saxena Kul, strategies for software-based hybrid business models, The Journal of Strategic Information Systems, 2012.

Haag Stephen et Cummings Maeve, Management Information Systems for the Information Age (8thed.). New York: McGraw-Hill/Irwin. 2010.

Hamel Jacques, Étude de cas et sciences sociales, Paris, L'Harmattan, 1997.

Hassenteufel Patrick, Sociologie politique: l'action publique, Armand Colin, 2008.

Hassenteufel Patrick et Smith Andy, Essoufflement ou seconde souffle ? L'analyse des politiques publiques à la française », Revue française de science politiques, 2002.

Harknett Richard, Callaghan John, Kaufmann Rudi: Leaving Deterrence Behind: Warfighting and National Cybersecurity, in, Journal of Homeland Security and Emergency Management, March 2010.

Hilgartner Stephen et Bosk Charles, « The Rise and Fall of Social Problems : A Public Arena Model », American Journal of Sociology, vol. 94, n° 1, 1988.

HALL Peter, « Policy Paradigm, Social Learning and the State », Comparative Politics, 1993.

Hlady-Rispal Martine, La méthode des cas : application à la recherche en gestion, Paris, De Boeck Université, 2012.

Hobbes Thomas, Leviathan, London, Oxford University Press, 1996.

Holleaux André, « Les lois de la troisième génération des droits de l'homme : ébauche comparative », Revue française d'administration publique, 1980.

Huet Philippe et Bravo Jacques, L'expérience française de rationalisation des choix budgétaires, , PRESSES UNIVERSITAIRES DE FRANCE, Paris, 1973.

Jönsson Alexandra, Dictionnaire des politiques publiques, Presse de Sciences Po, 2010.

Jones Charles, An Introduction to The Study Of Public Policy, Belmont, Wadsworth, 1970.

Jobert Bruno, Muller Pierre, L'Etat en action : politiques publiques et corporatismes , PUF, 1987.

Katzan Harry, On An Ontological View Of Cloud Computing, Journal of Service Science, 2010.

Kempf Olivier, Introduction à la cyberstratégie, Economica, 2015.

Kempf Olivier, L'affaire Snowden: Une rupture stratégique, Economica, 2015.

Kessler Marie-Christine, Les grands coprs de l'Etat, Paris, PuF, 1994.

Kingdon John, Agenda Alternatives and Public Policies, New York, Harper Collins, 1995, p.3).

Koenig Gérard, « Production de la connaissance et constitution des pratiques organisationnelles», Revue de l'AGRH, n° 9, novembre, 1993

Koubi Geneviève, « Responsabilisation des fonctionnaires et modernisation de l'administration », Revue administrative, n°284, 1 mars 1995.

Krasner Stephen, Sovereignty: Organized Hypocrisy, Princeton University Press, 1999.

KRANZBERG Melvin, Technology and History: "Kranzberg's Laws", Technology and Culture, Vol. 27, No. 1986.

Kübler Daniel et De Maillard Jacques, Analyser les politiques publiques, Presses universitaires de Grenoble, 2009.

Marx Karl, Contribution à la critique de l'économie politique, 1859.

Meddah Hassan, «Au FIC, Le Drian soigne sa cyberdéfense », L'Usine digitale, 22 janvier 2014.

Muller Pierre, De la théorie de l'État à l'analyse des politiques publiques, Que sais-je ? , 2009.

Müller Günter, Introduction of privacy and security in highly dynamic systems, Communications of the ACM, 2006.

Manovich Lev, Trending: The Promises and the Challenges of Big Social Data, Debates in the Digital Humanities, ed M.K.Gold, The University of Minnesota Press, Minneapolis, 2011.

Lachaumane Jean-François, La fonction publique, Dalloz, 1992.

La Palombara Joseph et Weiner Myron, Political Parties and Political Development apud Roger-Gérard Schwartzenberg, Sociologie Politique, Montchrestien, Paris, 1988.

Landry Réjean., Introduction à l'analyse des politiques publiques, Québec, Presse de L'Université de Laval, 1980.

Lange Oskar, « The Computer and the Market », in C. H. Feinstein (dir.), Socialism, Capitalism and Economic Growth, Cambridge, Cambridge University Press, 1967.

Lasswell Harold, Psychopathology and Politics, Chicago (Ill.), University of Chicago Press, 1930.

Lasswell Harold, A Pre-View of Policy Sciences, New York, American Elservier, 1971.

Lasswell Harold et Kaplan Abraham, Power and Society, A framework for Political Inquiry, London, Kegan Paul, 1952.

Laufert Romain et Burlaud Alain, Management Public, Gestion et Légitimité, Dalloz, 1980.

Leca Jean, Thoeing Jean-Claude, Grawitz Madeline, Traité De Sciences Politiques : politiques publiques, Tome 4, PUF, 1985.

Leca Jean, « La gouvernance de la France sous la Vème république. Une perspectives de sociologie comparative » , Paris, Presses de Sciences Po, 1996.

Le Crosnier Hervé , Schaefer Valérie et Musiani Francesca, La neutralité de l'Internet : enjeux de communication, CNRS édition, 2011.

LEFORT Claude, Essais sur le politique. XIXe-XXe siècles, Le Seuil, Paris, 1986.

Le Fur Louis, État fédéral et confédération d'états, Marchal et Billard, 1986.

Le Galès Patrick, « Gouvernance », Dictionnaire des politiques publiques, Paris, Presses de Sciences Po (P.F.N.S.P.), «Références », 2010.

Le Moigne Jean-Louis, Les Épistémologies constructivistes, Paris Presses Universitaires de France, Que sais-je ? , 1995.

Lemoine Simon, Le sujet dans les dispositifs de pouvoir, Press Univ de Rennes, 2013.

Le Pors Anicet, « Du nouveau dans les relations administration-citoyens », in AJDA, n°12, pp. 626-62, 26 mars 2007.

Leiner Barry , Cerf Vinton, Clark David, Kahn Robert, Kleinrock Leonard, Lynch Daniel, Pstel Jon, Reberts Larry, Wolff Stephen, A Brief History of the Internet, 2003.

Lerner Daniel et Lasswell Harold, The policy Sciences, Recent development in Scope and Method, Stanford University Press, 1951.

Levy Pierre, L'intelligence collective. Pour une anthropologie du cyberespace. Paris: La Découverte, 1994.

Libicki Martin, Crisis and Escalation in Cyberspace, Santa Monica, Rand, 2012.

LindBlom Charles et Woodhouse Edward, The policy making Process, Prentice Hall, p.11, 1993.

Lin Angela et Chen Nan-Chou, Cloud computing as an innovation: Perception, attitude, and adoption, International Journal of Information Management. 2012.

Locke. John, Traité des gouvernements civil (1690), Flammarion, 2000.

Negrier Emmanuel, L'analyse comparée des politiques publiques : Méthodes et principes vécus, De Boeck Sup, 2005

Nilsson Nils, Artificial Intelligence: A New Synthesis, Morgan Kaufmann, 1998.

Machiavel Nicolas, Le Prince (1532) – Réédition, Le prince : Texte intégral analyse, N. Machiavel, T. Ménissier, Poche, 2003.

Marsh David et Stocker Gerry,« Theory and Methods in Political Sciences», Basingstoke: McMillan Press, 1995.

Mattelart Armand, La Globalisation de la surveillance, Paris, La Découverte, 2007.

Mattelart Armand, Histoire de la société de l'information, Paris : La Découverte, 2001.

Mell Peter et Grance Tim, the NIST Definition of Cloud Computing, NIST, 2011.

Mény Yves et Thoeing J-C, Politiques publiques, Paris, PUF, 1989.

Ministère des finances, Rapport « Economique, social et financier :Projet de loi de finances pour 2009 », 2009.

Miles Matthews et Huberman Mickael, Analyse des données qualitatives, De Boeck Supérieur, 2003

Miles Matthews et Huberman Mickael, « Data Management and Analysis Methods », London, Sage Publications, 1998, p. 179-210.

Mondoux André, « Identité numérique et surveillance », Les cahiers du numérique, no 1, pp.1-13, 2011.

Mounier Pierre, Les maitres du réseau : les enjeux politiques d'INTERNET, La découverte, Paris, 2002.

Modeen Tore, « La protection des droits de l'homme et le rôle des administrations en Finlande », in Revue internationale de droit comparé, n°3, 1 juillet 1995, pp. 659-679.

Mueller Milton, Networks and stats: The global politics of Internet governance, MIT Press, 2010.

Mueller Milton, Ruling the root : Internet governance and the taming of cyberspace, MIT Press, 2002.

Muller Pierre, De la théorie de l'État à l'analyse des politiques publiques, Que sais-je ? , 2009.

Muller Pierre et Surel Y, L'analyse des politiques publiques , Paris : Montchrestien, 1998.

NABIL AHMED, Reaching for the "cloud": How SMEs can manage. International Journal of Information Management, 31, 272-278. 2001.

Lachaume Jean-François, La fonction publique, Dalloz, 1992.

Landry Réjean, Introduction à l'analyse des politiques publiques, Québec, Presse de L'Université de Laval, 1980.

Laurent Marilyne et Saoussane Bouzefrane, La gestion des identités numériques, Londres, ISTE, 2015

Nollet Jérémie, « Croiser analyse des politiques publiques et sociologie des médias : genèses et usages des concepts de mise à l'agenda et de construction des problèmes », communication au Xe congrès de l'Association française de science politique, Grenoble, 2009.

Nye Joseph, The Futur of the Power , Public Affairs, U.S.A , 2011.

OCDE, Panorama des administrations publiques, 2013.

Olson Mancur, Logique de l'action collective, Paris, PUF, 1978.

Oliveira Tiago, Thomas Manoj et Espadanal Mariana, Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. Information & Management, 497-510. 2014.

Osterwalder Alexander et Yves Pigneur, Business model generation: A handbook for visionaries, game changers, and challengers, Wiley. 2010.

Ouazzani Chahidi Hassan, Droit administratif, Najah El Jadida, Casablanca, 2003.

Paioleau J-G, L'Etat au concret, Paris, PUF, 1982.

Padioleau Jean, La mise en œuvre des politiques publiques, Paris ,1978.

PERIES Gabriel, La confiance au prisme de la « sécurité nationale». Une analyse critique à l'ère des réseaux numériques, Politiques sécuritaire et surveillance numérique, P-A CHARDEL (Coord), Paris, Hermès, 2014, P.59.

Pécheul Armel, La souveraineté dans tous ses états, Edition Cujas, Paris, 2011.

Perret Veronique et Séville Girod, Fondements épistémologiques de la recherche, dans Méthodes de recherche en management, Paris , Dunod, 2007.

Piaget Jean, Logique et connaissance scientifique: les courants de l'épistémologie scientifique contemporaine. Paris, Presses Universitaires de France, 1967.

Pontier Jean-Marie, les services publics , Hachette, 1996.

Pollitt Christopher et Bouckaert Geert, Public Management Reform: A Comparative Analysis, OUP Oxford, 2004.

Plouin Guillaume, Cloud computing, Une rupture décisive pour l'informatique d'entreprise, Paris, Dunod, 2011.

Pressman Jeffrey et Wildavski Aaron, Implementation politics policies, 1973.

Proulx Serge, L'irruption des médias sociaux: enjeux éthiques et politiques, Presses Universitaires du Québec, 2012.

Quermonne Jean-Louis, Le système politique de l'Union Européenne, Montchrestien, 2005.

Rapport de la Commission Européenne, Le défi numérique européen, Octobre 2013.

Rich Elaine , Knigh Kevin , Artificial Intelligence, McGraw Hill Inc, 1991.

Roché Sébatien, Police de Proximité, Paris Seuil, 2005.

Raynaud Philippe et Rials Stéphane, Dictionnaire de philosophie politique, Paris, PUF, 2003.

Rosa Hartmut, Aliénation et accélération. Vers une théorie critique de la modernité tardive, Paris, La Découverte, 2012.

Rose Richard, Inertia effects, in A. Groth et L. Wade (eds), Comparative Resource Allocation. Politics, Performance, and Policy Priorities, Beverly Hills (California), Sage Edition, 1984.

ROUSSEAU Jean-Jacques, Du contrat social, Paris, Flammarion, 2001.

Rousset Michel, Jean GARAGNON, Droit administratif marocain, Ed. La porte, octobre 2003.

Royer Isabelle et Zarlowski Philippe, « Le design de la recherche », dans Méthodes de recherches en management, Paris, Dunod, 2007.

Rose Richard, Davies Philip, Inheritance in Public Policy : Change without Choice in Britain, New Haven : Yale University Press, 1994.

Rule James, « Deux parcours divergents : les climats politiques et l'accessibilité croissante des renseignements personnels », Actes du 14e colloque du Creis, Paris, juin 2007.

Rouban Luc, Ziller Jacques, « De la modernisation de l'administration à la réforme de l'Etat », in Revue française d'administration publique, n°75, juillet-septembre 1995.

Sabatier Paul, « The need of better theories, in P. Sabatier (Ed.), Theories of the policy process, Boulder, Col, Wester View Press, 2007.

Savage Steve, Police Reform, Forces for Changes, Oxford University Press, 2007.

Santo Viriato-Manuel et Verrier Pierre-Éric, Le management public, Paris, Presse Universitaire de France, 2007.

Schutz Alfred Contribution à la sociologie de l'action, Broché, 2009.

Serres Michel, Petite poucette , Paris, Editions le Pommier, 2012.

Shivakumar Raju, Emergence role of Cloud Computing in redefining business operations, Global Management Review, 4(4), 48-52. T. 2010.

Simon Alexander, Models of bounded rationality, Cambridge : MIT Press, 1982-1997.

Simon Alexander, Administrative behavior: a Study of Decision-Making Processes in Administrative Organizations, New York : The Free Press, 1997.

Solum Lawrence, Models Of Internet governance, In Bygrave, L et Bing J 5Eds), Internet Governance: Infrastructure and Institution, 2009.

Sultan Nabil, Discovering the potential of cloud computing in accelerating the search for curing serious illnesses, International Journal of Information Management, 2014.

Sultan Nabil, Knowledge management in the age of cloud computing and Web 2.0: Experiencing the power of disruptive innovations. International Journal of Information Management, 33, 160-165. 2013.

Smith Adam, An Inquiry Into Nature And Causes Of The Wealth Of Nations, 1776, republié par Edwin Cannan In University Paperbacks, Methvnen & C, Ltd, London, 1961.

Taylor Charles, The Malaise of Modernity, Anansi, 1991.

Teneyuca David, Internet cloud security: The illusion of inclusion, Information Security Technical Report, 2011.

Tétu Jean-François, Pierre Musso, Saint-Simon, l'industrialisme contre l'État, Paris, Éd. de l'Aube, 2010.

Thoeing Jean-Claude, Grawitz Madeline, Leca Jean, Traité De Sciences Politiques : politiques publiques, Tome 4, PUF, 1985.

Thietart Raymond-Alain, Méthodes de recherches en management, Paris, Dunod, 2007.

The Economist ,« Data, Data Everywhere. Special Report : Managing Information », 25 février. 2010.

Tounay Virginie, La sociologie des institutions : Une sociologie processuelle, PUF, 2011

Usunier Jean-Claude, Introduction à la recherche en gestion, Paris, Economica, 1993.

Vaquero Luis, Rodero-Merino Luis, Caceres Juan et Lindner Maik, A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review, 2008.

Vakil Farok et Lu Victor et Russakoff Andrew, Recent Developments in Cloud Computing and High Speed Connections for Business Practices. Review of Business. 2012.

Vitalis André, «Informatique et libertés » : une histoire de trente ans, C.N.R.S. Editions, 2009.

Voirol Olivier, Les luttes pour la visibilité : Esquisse d'une problématique, La Découverte, 2005.

Yin Robert Case Study Research: Design and Methods,SAGE Publications, 2003

Yves Mény et Jean-Claude Thoenig, Politiques publiques, UF, 1989.

Ye Nong, Yang Su et Aranda Billibaldo, The analysis of service provider-user coordination for resource allocation in cloud computing. [Article]. Information Knowledge Systems Management, 2013.

Wacheux Frédéric, Méthodes Qualitatives Et Recherches En Gestion, Paris, Economica, 1996.

Wasmer Etienne et Ferracci Marc, État moderne, état efficace, Odile Jacob¸ 2011.

Waxer Nathan., Ninan David, Ma Alfred, Dominguez Norma, Continuous Quality Monitoring through Analytics and Cloud Computing. Physician Executive, 2013.

Waterbury John, « Le commandeur des croyants, la monarchie marocaine et son élite», PUF, 1975.

Weber Max, Le Savant et le Politique, La Découverte, 2003.

Weber Max, Economie et Société, Pocket, 2003.

Westin Alan, Privacy and freedom, New York. USA. 1967.

Weiner Mervyn, « Amélioration de la gestion fédérale au Mexique : Essai sur une réforme institutionnelle », in Revue internationale des sciences administratives, 1987.

Wiener Norbert, « Cybernétics or control and communication in the animal and machine», 1948.

Wiener Norbert, The Human Use of Human Beings, 1950.

Wildavsky Aaron, Budgeting. A Comparative Theory of Budgetary Process, Boston (Mass.), Little, Brown and Co, 1975.

William James, « Le pragmatisme et le sens commun. », Sociétés 3/2005 (no 89) , p. 29-42

Wilson Larsen, Interest Group Politics in France, Cambridge University Press, 1987.

Wilson Larsen, « Alternative Models of Interest Intermediation: the Case of France », British Journal of Political Science, Avril 1982, p. 173-200

Winston Patrick-Henry, Artificial Intelligence, Third Addition: Addison-Wesle, 1992

Wired Magazine, 2008, http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory, dernière consultation (08 Mai 2015).

Ziller Jacques, « De la modernisation de l'administration à la réforme de l'Etat », Revue française d'administration publique, n°75, juillet-septembre 1995.

Annexes

VI. Annexes

1 Glossaire : sigles

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

AFNIC : Association Française pour le Nommage Internet en Coopération

ARCEP : Autorité de Régulation des Communications Electroniques et des Postes

ARPANET: Advanced Research Projects Agency Network

BYOD: Bring Your Own Device

CDO: Chief Data Officer

CERN : Organisation Européenne pour la Recherche Nucléaire

CNDP: Commission Nationale de Protection des Données Personnelles

CNCIS: Commission nationale de contrôle des interceptions de sécurité

CNCTR: Commission nationale de contrôle des techniques de renseignement

CGEM : Confédération générale des entreprises du Maroc

DGFP : Direction Générale des Finances Publique

DARPA: Department of Advanced Research Projects Agency

DPR : Délégation Parlementaire au Renseignement

DNS: Domain Name System

FAI : Fournisseurs d'accès Internet

FCA : Fournisseurs de Contenus et d'Applications

FGI : Forum sur la gouvernance de l'Internet

IaaS: Infrastructure As A Service

IETF: Internet Engineering Task Force

ICANN: l'Internet Corporation for Assigned Names and Numbers

IESG: L'Internet Engineering Steering Group

IP: Internet Protocol

IoT: Internet of Things

ISOC: l'Internet Society

IAB: L'Internet Architecture Board

IUT: International Telecommunication Union

LOLF: La loi organique relative aux lois de finances

LPM : Loi de Programmation Militaire

MAP: Modernisation de l'Action Publique

MOOC: Massive Open Online Course, MOOC

NSA: National Security Agency

NIST: National Institute of Standards and Technology

OCDE: Organisation de Coopération et de Développement Economiques

OMC : Organisation Mondiale du Commerce

PaaS : Plateforme As A Service

PATRIOT Act: Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

RGPP : Révision générale des politiques publiques

RFC: Requests for Comments

SaaS: Service As A Service

SMSI : Sommet Mondial sur la Société de l'Information

SGFP : Statut Général de la Fonction Publique

SWIFT: Society for Worldwide Interbank Financial Telecommunication

TTIP: Transatlantic Trade and Investment Partnership

TISA: Trade in Services Agreement

TCP: Transmission Control Protocol

VTC : Voiture de tourisme avec chauffeur

W3C: World Wide Web Consortium

2 Tables des figures et tableaux

Liste des Figures

- Figure 1 : Présentation NIST de modèle Cloud Computing
- Figure 2 : Objectifs visés par la mise en place d'un nouveau système d'information de l'État unifié
- Figure 3 : Schéma représentant l'approche séquentielle d'analyse des politiques publiques
- Figure 4 : Objectifs visés de la migration vers le Cloud (extrait de l'étude KPMG)
- Figure 5 : Schéma illustrant les compétences d'un «data scientist»
- Figure 6 : la hiérarchie des noms de domaine pour Wikipédia
- Figure 7 : Répartition des RFCs déposées par acteurs (Entreprises et universités)
- Figure 8 : Schéma des principales mesures du plan Big data
- Figure 9 : Historique d'adoption de la loi croissance et compétitivité
- Figure 10 : Historique d'adoption de la loi relative au renseignement
- Figure 8 : Répartition des acteurs autour d'Internet (selon Fayon)
- Figure 9 : Calssement des pays selon les entreprises numérique et leurs chiffres d'affaire (selon Fayon)
- Figure 10 : Carte officielle du Maroc issue de http://www.sahara.gov.ma/

Liste des tableaux

- Tableau 01 : Position épistémologique et Paradigmes de recherche
- Tableau 1 : Liste des différentes définitions de Cloud Computing
- Tableau 2 : Comparaison des deux solutions d'hébergement : Cloud et On-premise
- Tableau 3 : Synthèse du projet Cloudwatt avec utilisation des neuf blocs de la matrice proposée par Osterwaler et Pigneur (2010)
- Tableau 4 : Synthèse de Numergy avec utilisation des neuf blocs de la matrice proposée par Osterwaler et Pigneur (2010)

Liste des schémas

- Schéma 01 Gestion de budget à travers de l'application « Balancing Act »
- Schéma 02 : Origines des ressources dans l'application « Balancing Act »
- Schéma 03 : Comparaison des budgets dans l'application « Balancing Act »
- Schéma 04: Comparaison des budgets dans l'application « Balancing Act »
- Schéma 05 : Affichage des dépenses dans l'application « Balancing Act »
- Schéma 06 : Origines des ressources dans l'application « Balancing Act »
- Schéma 07 : Affichage du récapitulatif dans l'application « Balancing Act »

3 Liste des différentes définitions de Cloud Computing

Auteur	Definitions de Cloud Computing
Vaquero (2008)	"Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs." *" Le Cloud est un ensemble de ressources facile à utiliser et à accéder (comme le matériel, les plateformes de développement et de services). Ces ressources sont configurables dynamiquement pour s'adapter à une charge variable (Scale), ce qui permet une optimisation d'utilisation des ressources. Ce regroupement de ressources est typiquement exploité par un modèle du paiement à l'utilisation pour lequel le fournisseur d'infrastructure garanti des SLA spécifiques ».*
Birman (2008)	"From the outward-looking perspective of an end user looking at the cloud, it shifts functions that used to be performed by computers located at the network's edge (such as hosting software and data) into data centers residing in the network's core. From the inward-looking perspective of how individual cloud computing elements interact with other cloud computing elements, the focus is on the ability to coordinate and integrate applications and data operating on multiple machines through mechanisms into a seamless whole." *" depuis une perspective extérieure d'un utilisateur final, le coud transfère les fonctions réalisées habituellement par des ordinateurs localisés au bord d'un réseau (exemple hébergement de logiciel et donnée) vers des centres de données situé au cœur du réseau. Depuis une perspective intérieure, la façon dont les éléments de cloud computing interagissent individuellement avec d'autres éléments de cloud computing consiste dans la capacité à coordonner et intégrer, à travers des mécanismes, les applications et les données qui s'exécutent dans plusieurs machines vers un ensemble homogènes »*
Buyya (2009)	"A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers." (p. 601)

	"Le cloud est un système parallèle et distribué qi consiste à collecter des machines interconnectées et virtualisés qui sont dynamiquement provisionnées et présentées comme une ou plusieurs ressources informatiques en se basant sur le niveau de qualité établi et négocié entre le fournisseur Cloud et les clients " (p.601)
Armbrust (2009)	"Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud." *"Le Cloud computing fait référence à la fois aux applications livrées en tant que service à travers Internet, au matériel et aux systèmes logiciels fournis dans un même centre de données. Les services eux-mêmes ont toujours fait références au logiciel à la demande. Le matériel et le logiciel du centre de données c'est ce qu'on appellera le cloud »*
Chen	"Cloud computing is an emerging business model that delivers computing services over the Internet in elastic self-serviced, self-managed, cost-effective manner with guaranteed Quality of Service (QoS)." " Le Cloud Computing est un modele métier emergent qui permet de fournir des services informatique a travers Internet d'une facon elastiqe, auto-géré à oindre cout tout en respectant une qulaité de service"
Haag et Cuming (2010)	"Cloud computing is a technology model is which any and all resources-application software, processing power, data storage, backup facilities, development tools… literally everything-are delivered as a set of services via the Internet." "Le Cloud Computing est un modèle technologique qui permet de fournir sous forme de service des ressources applicatives logicielles, puissance de traitement, de stockage de données, des facilités de sauvegarde à travers Internet »
Chang (2010)	"Cloud Computing aims to provide scalable and inexpensive on-demand computing infrastructures with good quality of service (QoS) levels. More specifically, this involves a set of network-enabled services that can be accessed in a simple and pervasive way." "Le Cloud Computing a pour objectif de fournir des ressources informatiques extensible de bonne niveau de qualité de service. Cela implique des services basés sur un accès facile via le réseau »

Katzan Jr, H. (2010)	"Cloud computing is an architecture for providing computing service via the Internet. Cloud computing is a means of providing computer facilities via the Internet, but that is only half of the picture. The other half is that it is also a means of accessing those same computer facilities via the Internet from different locations." "Le Cloud Computing est une architecture qui permet de fournir un service de calcule via Internet. Le Cloud Computing signifie fournir des facilités de calcul via Internet en partie. L'autre partie signifie que l'accès a ses services de calcule peuvent se faire depuis plusieurs endroits géographiques »
Shivakumar et Raju (2010)	"Cloud computing is a simple style of computing in which massively scalable IT-enabled capabilities are delivered 'as a service' to multiple customers using internet technologies, Cloud computing can be positioned as a business enabler." "Le Cloud Computing est une sorte de calcule dans lequel les capacités IT sont scalable et fourni en tant que service à plusieurs client a travers de technologies Internet. Le Cloud Computing peut se positionner comme un nouveau modèle d'affaire »
Mell et Grance (2011) NIST	"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. This cloud model is composed of five essential characteristics, three service models, and four deployment models." « Le Cloud Computing est un modèle qui permet un accès pratique aux ressources informatiques partagées et configurables (par exemple, réseaux, serveurs, stockage, applications et services) et qui peuvent être provisionnés rapidement avec un minimum d'effort sans interaction avec le fournisseur. Ce modèle est composé de cinq caractéristiques essentielles, trois modèles de services et quatre modèles de déploiement »
Chonka (2011)	"Cloud computing systems are providing a wide variety of services and interfaces to enable vendors to rent out spaces on their physical machines at an hourly rate for a tidy profit. The services that are provided by these vendors can vary from dynamically virtual machines to flexible hosted software services. Each machine and software shares the notion that delivered resources should be allocated and de-allocated on demand, at the same time as providing reasonable performance." "Les systèmes Cloud Computing sont fournissent une variété de services et interfaces qui permettent aux vendeurs de louer des espaces dans leurs machines physique à l'heure. Ces services fournies par les vendeurs peuvent être différents de machines virtuelles jusqu'aux services logiciels. Toute machine ou logiciel partage la notion des ressources fourni et loué ou dé loué à la demande en même temps qu'un service raisonnable de performance »

Nabil Ahmed, S. (2011)	"The definition that describes it as clusters of distributed computers (largely vast data centers and server farms) which provide on-demand resources and services over a networked medium (usually the Internet) seems to be commonly accepted." "La définition la lus acceptée est celle qui décrit le Cloud Computing est une grande distribution des machines de calcules (des grands centre de données) qui fournissent des ressources et services à la demande via un réseau (souvent Internet) »
David, T. (2011)	"The cloud computing technology allows business owners and consumers access to all sort of applications and their personal files over the Internet, without them installing any files at a computer with Internet access." " La technologie de Cloud Computing permet aux chargés d'affaires et aux clients d'accéder à un ensemble des applicatons et leurs fichier à travers l'Internet sans les installer »
Espadas (2011)	"Cloud computing refers to both the applications delivered as services over Internet and the hardware and systems software in the datacenters that provide those services commonly in a pay-per-use pricing basis. With cloud computing definition comes the term of elasticity which is the ability to create a variable number of virtual machine instances depending on the applications demands." "Le Cloud Computing renvoie vers les applications fourni comme service à travers Internet, et aussi du matériel et de logiciel dans des centres de données fournissent ces services dans un modèle de paiement à l'utilisation. Avec la définition de Cloud Computing contient aussi la notion de l'élasticité qui signifie la capacité à créer des un nombre de machines virtuelles selon les applications demandés. »
McAfee, A. (2011)	"Cloud computing is a sharp departure from the status quo. Today most companies own their software and hardware and keep them "on premise" in data centers and other specialized facilities. With cloud computing, in contrast, companies lease their digital assets, and their employees don't know the location of the computers, data centers, applications, and databases that they're using. These resources are just "in the cloud" somewhere." "Le Cloud Computing est partie d'un statut quo. Aujourd'hui, une grande majorité des entreprises détiennent leurs propres logiciels et matériels hébergées dans leur propre centre de données avec un certain nombre de certaines. Avec le Cloud Computing, les entreprises louent les biens et les employées ne reconnaissent pas l'emplacement de ces machines, centres de données, et applications et les bases de données utilisées. Ces ressources sont seulement quelque part dans le Cloud »

Youssef et Alaqeel (2011)	"A Cloud can be viewed as a pool of services provided by a cloud service provider (e.g., Google, Yahoo, Salesforce) who can be regarded as a company that leases to its customers a number of reliable virtual resources (hardware or software of any kind) according to a certain business model. Cloud service providers deliver general business applications online that are accessed from a Web browser, while the software and data are stored on the cloud servers." " Le Cloud peut être considéré comme un ensemble partagé de service fournie par fournisseur cloud (exemple google, yahoo, salesforce) qui peuvent être considérés comme des entreprises qui louent aux clients un ombre de ressources virtuel (matériel ou logiciel) selon un certain modèle d'affaire. Les fournisseurs de cloud fourni en général des applications accessible en ligne via un navigateur web pendant que les applications et le logiciels sont hébergés dans serveurs dans le cloud »
Khorshed (2012)	"Cloud Computing is a system, where the resources of a data centre is shared using virtualization technology, which also provide elastic, on demand and instant services to its customers and charges customer usage as utility bill." " Le Cloud Computing est un système où les ressources d'un centre de données sont partagées en utilisant la technologie de virtualisation qui permet de fournir une élastique et à la demande des aux clients qui seront payés à l'usage"
Hon (2012)	"Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand. Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers. Charging, where present, is commonly on an access basis, often in proportion to the resources used." "Le Cloud Computing fournie des ressources de calcules indépendante de leur localisation et qui sont provisionnés rapidement à la demande. Les services (spécialement les ressources) sont virtualisées alloué a un ensemble partagé de ressource pour d'autres clients. La paiement se fait selon la portion des ressources utilisées »
Lin et Chen (2012)	"Cloud' is metaphorical and typically points to a large pool of usable resources such as hardware and software that are easily accessible via the Internet." "Le Cloud renvoie métaphoriquement à un large ensemble des ressources matérielles et logicielle facilement accessible à travers Internet"

von Solms et Viljoen (2012)	"Cloud computing is a computing model which allows one to access an IT service over a network, as or when it is needed, without worrying about the technical details of how the service is provided." "Le Cloud Computing est un modèle de calcul qui permet un seul accès aux services IT à travers un réseau quand c'est besoin sans se soucier des détails techniques sur le façon dont ces ressources sont fournies."
Dutta (2013)	"Cloud computing is an advanced IT model to host and share both software and hardware resources over the Internet. It allows organisations to use a pool of IT resources and applications as services virtually through the web, without physically holding these computing resources internally." " Le Cloud Computing est un modèle IT avancé pour héberger et partager chacune des ressources logicielles et matérielles a travers Interner. Il permet aux organisations d'utiliser un ensemble des ressources et des applications comme des services virtuelles via le web sans avoir physiquement ces ressources en interne. »
Gupta (2013)	"Cloud computing (dependent variable) is similar to an electric-ity grid, where resources like hardware, software, information arepooled and shared with the end-user via the internet, which is usedas a medium of exchange. Users do not know theexact location of their digital data. The frame work provided by cloud computing is in the form of high quality leased IT resources instead of building the IT infrastructure from scratch." "*Le Cloud Computing (une variable dépendante) est similaire a ne grille d'électricité ou les ressources comme le matériel, le logiciel et les informations sont partagés entre les utilisateurs à travers Internet qui est utilisé comme un moyen d'échange. Les utilisateurs ne connaissent pas la localisation exactes des de leurs données numériques. Les outils de travail fourni par le Cloud Computing est dans une forme de location de ressources IT au lien de leur création à partir de rien* »
Ye (2013)	"A cloud is a pool of virtual computing, data and software resources that are built on a distributed infrastructure of physical resources and are accessed via the network or Internet. Cloud computing is to provide on-demand IT services to users who pay for the usage of virtual resources." " *Le Cloud est un ensemble des ressources virtuelles, données et logiciels, qui sont créés dans une infrastructure de ressources physiques partagées et accessibles par un réseau ou Internet. Le Cloud Computing c'est fournir des services IT à la demande à des utilisateurs qui payent à l'usage des ressources virtuelles*. »
Sultan, N. (2013)	"Cloud computing is a model of delivering a range of IT services remotely through the Internet and/or a networked IT environment." " Le Cloud Computing est un modèle de fournture de services IT à distance et à travers Internet ou un environnement réseau IT"

Waxer et al. (2013)	"Cloud computing is essentially an Internet-based system where files, data and applications can be shared by any authorized user with Web access." " Le Cloud Computing est modèle de livraison d'un ensemble de service IT à distance et à travers l'Internet ou/et un environnement réseau IT" « *Le Cloud Computing est essentiellement basé sur Internet ou les fichiers, les données et les applications peuvent être partagés entre des utilisateurs à travers un accès web* »
Marešová et Půžová (2014)	"Cloud computing is a broad and highly innovative approach, representing the transfer of traditional IT services to the new business model – the so-called cloud, which represents a unique area with new business opportunities and models." *"Le cloud Computing est une approche large et très innovante qui représente le transfert des services informatiques classiques vers un nouveau modelé économique. Le présupposé Cloud représente un environnement des nouvelles opportunités et modèles économiques. «*
Oliveira (2014)	"Cloud computing evolved through the recent advancements in hardware, virtualization technology, distributed computing, and service delivery over the Internet. The ''cloud'' metaphor is a reference to the ubiquitous availability and accessibility of computing resources via Internet technologies." *"Cloud computing a évolué à travers les récents progrès dans le matériel, la technologie de virtualisation, l'informatique distribuée, et les services fournies par Internet. Le métaphore « Cloud » fait référence à la disponibilité permanente et accessibilité des ressources informatiques à travers les technologies de l'Internet »*
Sultan, N. (2014)	"Cloud computing is an IT solution and a business model that uses advances in ICT technologies such as virtualization and grid com-puting to remotely deliver (on demand) a range of ICT services (e.g.,business and development software, processing power, storage) through the Web and other media such as a network infrastructure. The cloud paradigm is different in the sense that a physical product (e.g., software and hardware) is transformed into a service." "*Cloud Computing est une solution informatique et un modèle économique qui permet d'utiliser les avancées des technologies de l'information et de la communication comme la virtualisation et l'informatique pour fournir à distance et à la demande un ensemble des services TIC (exemple des logiciels métier, puissance de traitement, stockage) à travers le web ou autre canal comme l'infrastructure réseau. Le paradigme de Cloud est différent dans le sens où un produit physique (logiciel et matériel) est transformé en un service.* »

4 Liste des personnes interviewées acceptant d'apparaitre sur notre annexe :

Nicolas Monserrat	Responsable de secteur Service public France chez Accenture
Marc Bousquet	Associé Accenture et expert Cloud pour le secteur public France
Dominique Tessaro	Directeur des systèmes d'information VINCI
Nasser Kettani	Directeur technologique Microsoft pour Moyen Orient et Afrique
Arnauld Lefaive	Directeur Numergy - France
Said Lhrai	Directeur de la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel au Maroc
Kiet Truong	Architecte Cloud chez SAP France

5 Liste des travaux réalisés

5.1 Colloque : l'efficacité collective à l'ère numérique

Ce colloque fait suite à notre participation en tant que consultant et doctorant aux travaux et ateliers coordonnés par la prospectiviste Carine Dartiguepeyrou. Et à l'occasion de la publication de son cahier de prospective sur l'efficacité collective à l'ère numérique, issu des travaux du Think Tank de l'Institut Mines-Télécom, mon intervention portait principalement sur le rôle de la génération Y dans l'efficacité collective et comment cela s'articule au sein des organisations. Ce colloque a été principalement animé par la Fondation Telecom, Orange, SFR, Accenture (que je représentais), ENGIE (ex GDF Suez) ainsi que plusieurs startups venant partager le rôle du numérique dans le développement des territoires. Concrètement, j'ai articulé mon intervention sur trois principaux :

- La génération Y et le numérique
- La génération Y et le numérique au sein des organisations
- L'avenir numérique à partir du prisme de la génération Y.

Ce colloque a eu lieu le 08 Avril 2016 au sein de l'Institut Mines-Télécom à Paris.

5.2 Participation aux travaux de la chaire «Valeurs et politiques des informations personnelles» de l'Institut Mines-Télécom

Présentation des travaux aux membres de la chaire :

- Date : 06 Juin 2014
- Lieu Institut Mines-Télécom :
    - Description de la présentation :
    - Présentation du sujet de rechercher et les différents aspects à couvrir
    - Une revue de la littérature à ce stade de la recherche

Participation aux différents ateliers organisés par la chaire :

5.3 Séminaire « Gouvernance de données : Nouvelle pierre angulaire de la relation client du secteur bancaire ?»

- Lieu : Télécom Ecole de Management
- Date : Mai 2015
- Objectif : Ce séminaire avait pour objectif de discuter les enjeux liés à la donnée dans le secteur bancaire.

5.4 Séminaire « Décentralisation et vie privée : une voie européenne ? »

- Lieu : Ecole des Mines Paris
- Date : Juin 2015
- L'objectif de ce séminaire est de discuter les différents enjeux liés à la protection des données personnelles à l'échelle européenne.

5.5 Forum MEDays Tanger (Décembre - 2014)

Ce forum organisé à Tanger au Maroc en juin 2014 avait permis de rassemble un ensemble de décideurs méditerranéens pour discuter des différents enjeux contemporains.

Ma contribution consistait dans la participation aux deux ateliers suivants :

- Atelier: Technologies et Télécoms: Investir et innover pour assurer la croissance et la compétitivité.
- Atelier: Cyber Guerre et e-sécurité : Comment résoudre l'équation post-Snowden ?
- Lieur Tanger
- Date : Juin 2014

5.6 Séminaire « WebDays » - Université Blida Algérie

- Lieu : Blida – Algérie
- Date : Mars 2014
- Contribution : Ce séminaire était dédié à l'entreprenariat numérique. Ma contribution concernait l'animation de l'atelier : Entreprenariat et Mobilité. L'objectif était de montrer le lieu entre le Cloud, la donnée et la mobilité (smartphones) et quel écosystème forme les trois concepts avec l'ensemble des enjeux associés et indissociables
-

5.7 Autres séminaires :

- Innovatives SHS - Cité des sciences et de l'industrie (16 Juin 2015)
  - Table ronde: Les Big Data pour les Sciences Humaines et Sociales

- Bibliothèque Publique d'Information (BPI) - Centre Pompidou
  - Animation atelier numérique : Services administratifs dans le cloud – Mai 2015
  - Conférence: « Big Data, je n'ai rien à cacher » - Juin 2015

5.8 Formations suivies :

- Formations doctorales (Octobre & Novembre 2014):
    - Fondamentaux de recherche (LITEM)
- La journée des doctorants de LITEM – Evry – (Mars 2015)
    - Poster et présentation des travaux aux différents invités
- Bibliothèque National de France (BnF) – (Mars 2015)
    - Formation: Orientation de la recherche bibliographique pour les doctorants
- Formation Université Evry – Centre Pierre Naville – LITEM – SDS – (Juin 2015)
    - La recherche en Sciences Humaines et Sociales

5.9 Cours enseignés:

- +100h du cours enseignés sur l'année pendant la période de recherche
- Niveau: 1A et 2A (ingénieurs et managers)
- Etablissement :
    - Télécom Sud Paris TSP (Evry)
    - Telecom Ecole de Management TEM (Evry)
    - Institut Supérieur de Génie Appliquée IGA (Maroc : Centre Rabat et Marrakech)
- Thématiques abordées:
    - Bigdata, Cloud Computing, etc.
    - Politiques publiques et politiques de surveillance, etc.
    - Vie privée et protection des données personnelles

5.10 Autres activités académiques

- Cité parmi les contributeurs au rapport Ambition Numérique de CNNum (Conseil National du Numérique). J'ai principalement participé à la question de la modernisation de l'action publique ainsi que à la question de la souveraineté numérique
- Cité parmi les contributeurs à la conception du rapport « République numérique »
    - Animation blog personnel avec une réflexion sur l'organisation de l'Etat et la digitalisation de la société en générale. Lien http://said-elouazzani.blogspot.fr
- Présentation thèse en 180 secondes – Université d'Evry – (Mars 2015)
    - Compétition de présentation de thèse en 180 secondes

5.11 Article : Comment le Cloud peut-il booster la compétitivité des PME ?

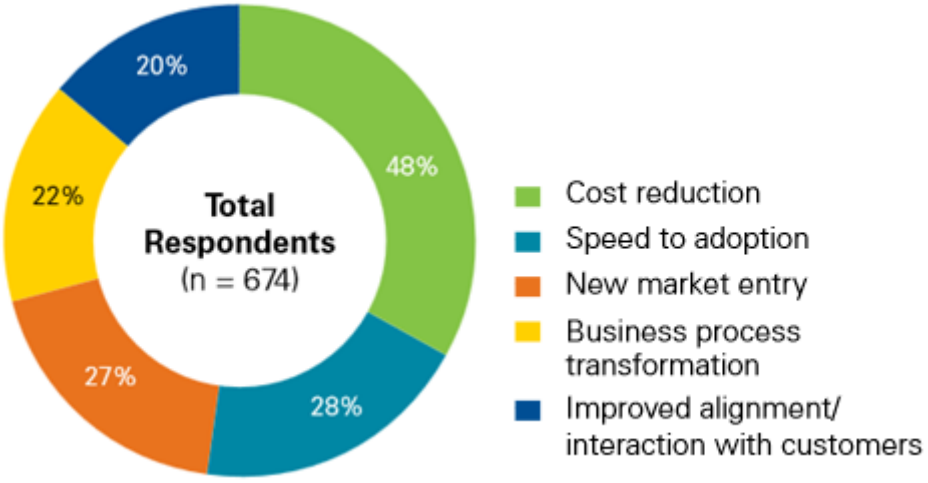
Comment le Cloud peut-il booster la compétitivité des PME ?

Par Saïd El Ouazzani

Paru sur HBR France :

http://www.hbrfrance.fr/chroniques-experts/2015/01/5779-comment-le-cloud-peut-il-booster-la-competitivite-des-pme/

L'adoption du Cloud Computing a connu une croissance fulgurante ces dernières années. Selon le cabinet IDC en 2012, le marché du Cloud a généré en France plus de 2 milliards d'euros de CA ; soit une croissance annuelle estimée à 25%. A l'échelle mondiale, le marché atteindra 241 milliards d'euros en 2020. Le Cloud constitue non seulement un enjeu stratégique mais également un enjeu de compétitivité économique pour les entreprises. D'après une étude(1) menée en 2013 dans 16 pays par le cabinet KPMG, la réduction des coûts (48%), la pénétration des nouveaux marchés (27%) et la transformation de l'activité (22%) apparaissent comme les principales motivations d'adoption du cloud pour les 674 décideurs IT interrogés. Dans un contexte mondialisé et concurrentiel, les PME sont amenées à considérer la technologie autrement et à se concentrer d'avantage sur leurs cœurs de métier.

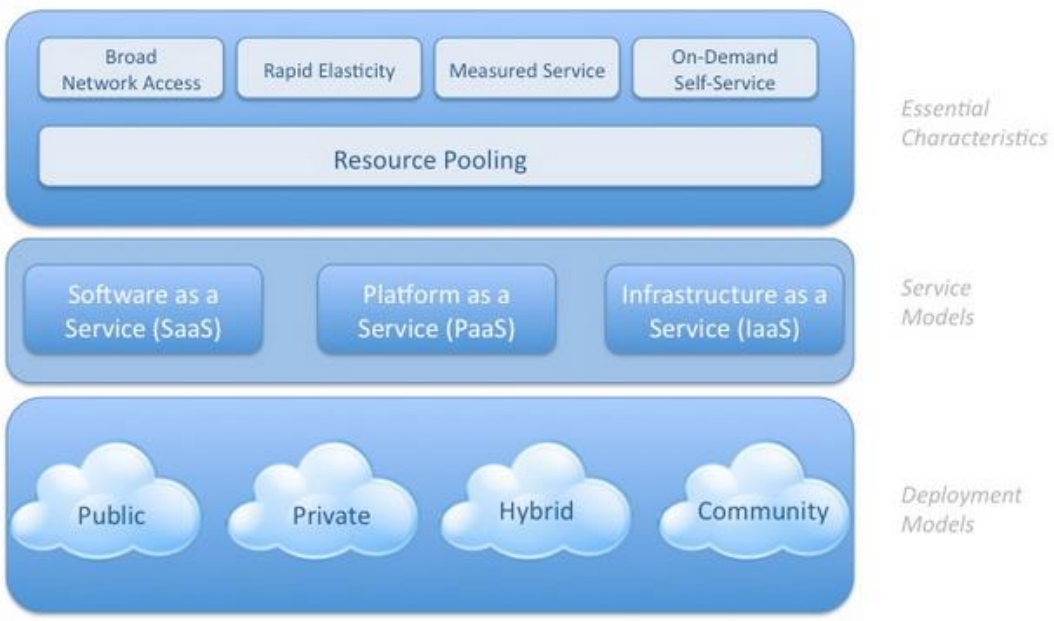


Objectifs visés de la migration vers le cloud (extrait de l'étude KPMG)

Définition de Cloud Computing :

Il existe plusieurs définitions de Cloud Computing, l'article intitulé « *A break in the clouds: Towards a cloud definition* »[(2)], paru en 2008, en recense vingt-deux. La définition la plus répandue est celle du National Institute of Standards and Technology. Le NIST, une agence du département du commerce extérieur des États-Unis, définit le Cloud Computing comme étant : *«l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées et configurables* » (Peter Mell and Tim Grance, 2009, P 2)**.** Le plus important dans ce qu'elle apporte la NIST est la grille de lecture du Cloud qui suit, avec ces éléments :

- Trois modèles de service : Software as a Service (SaaS), Plateforme as a Service (PaaS) et Infrastructure as a ervice (IaaS).
- Quatre modèles de déploiement : Public, privé, hybride et communautaire.
- Cinq caractéristiques : des services à la demande, des services mesurés, une bande passante élevée, un partage des ressources informatiques, et une élasticité et une flexibilité des ressources.



Grille de lecture du modèle NIST

En France, la commission générale de terminologie et de néologie, dont la mission est de favoriser l'enrichissement de la langue française, définit le Cloud Computing comme étant un « *mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire* ». Cette définition est apparue dans le journal officiel n°0129 du 6 juin 2010.

La définition du Cloud Computing se résume aux principes suivants:

- Une consommation des services à travers Internet, telle que la messagerie électronique (*Gmail, Hotmail, Yahoo mail, etc.).*
- Une gestion abstraite du logiciel ou du matériel d'un point de vue client. Ce dernier se concentre sur son cœur de métier et sous-traite cette gestion technique à des prestataires spécialisés.
- Un libre accès aux ressources informatiques, via Internet, depuis n'importe où et à tout moment avec un paiement flexible selon la consommation.

L'adoption de Cloud par les PME :

Les PME représentent une composante essentielle de l'économie nationale. Elles se caractérisent par leurs capacités de résilience, d'investissement continu et d'innovation (*un tiers des brevets est détenu par les PME, selon l'observatoire de la propriété intellectuelle*). Elles peuvent améliorer leurs performances en faisant appel à des services disponibles dans le Cloud. Selon une étude[(3)] réalisée par Microsoft, 59% des PME, consommatrices de ce type de services, ont constaté une croissance de leur productivité. En effet, les services Cloud offrent plusieurs avantages aux PME et déchargent ces dernières des contraintes liées à la gestion de l'informatique. Ce constat est confirmé par l'étude de KPMG citée plus haut. Les services Cloud les plus sollicités par les entreprises interrogées sont ceux de la gestion des ressources humaines (57%), de la gestion de l'infrastructure IT (54%) et des outils de collaboration (53%). D'une manière générale, les entreprises font appel aux services suivants dans le Cloud :

- Les outils de productivité et de collaboration : messagerie électronique (e.g. la suite Office 365), réseaux sociaux d'entreprises (e.g. Yammer) ;
- Les sites Internet : portail intranet entreprise, sites web, etc ;
- Les services de stockage et de partage en ligne ;
- Les applications métier : Gestion de la relation client (CRM), gestion des ressources humaines (GRH), etc.

Néanmoins, la migration des services vers le Cloud représente des risques liés principalement :

- Aux problématiques de confidentialité des données ;
- A la fiabilité des fournisseurs du Cloud ;

- A la capacité de migration d'un fournisseur vers un autre, avec une reprise de l'historique des opérations.

Cas d'utilisation d'un service Cloud par une PME :

Afin d'illustrer l'apport d'un service Cloud pour une PME, prenons l'exemple de la mise en place d'un service de stockage des données métier : factures clients, fiches fournisseurs, etc.

Selon le modèle d'implémentation choisi par la PME, la mise en place de ce service de stockage implique les opérations suivantes :

Solution dite « On-premises » ou locale	Solution dans le Cloud
• Achat du matériel (Hardware) et des licences logicielles associées (Software) • Charges d'exploitation et de maintenance : mise à jour, sauvegarde, etc. • Une équipe technique compétente pour gérer cette infrastructure : technicien système par exemple • Rigidité : Si le besoin en termes de stockage augmente, il serait nécessaire de renforcer les ressources techniques et humaines	• Souscription à un service Cloud de stockage : Sharepoint de Microsoft par exemple • Le fournisseur prend en charge l'exploitation et la maintenance de la solution avec un support 24x7 • Flexibilité : La PME peut augmenter ou réduire les ressources selon ses besoins et payer selon sa consommation • La PME se décharge de cette activité technique et se concentre sur son métier

Nous remarquons qu'avec l'option Cloud :

- La PME loue le service au lieu d'acheter une solution propre. Elle contribue ainsi à transformer le capital en dépenses opérationnelles variables (Opex, par opposition au Capex).
- Le fournisseur est le responsable du service complet : mise en place, configuration, maintenance, etc. Ainsi, la PME n'a plus à se charger de la gestion technique.
- La PME gagne en flexibilité et en rapidité de mise en place.
- La PME peut améliorer sa stratégie «Go-to-Market».

Conclusion :

Le Cloud Computing, dans sa forme actuelle, impose un nouveau Business Model qui bouleverse le rôle de l'informatique au sein des entreprises. En outre, le Cloud favorise l'émergence d'un modèle orienté « service » basé sur l'utilisation d'Internet. Il devient alors une composante indispensable pour les entreprises. En s'inscrivant à des solutions dans le cloud, les entreprises s'affranchissent des coûts associés à la gestion informatique et se concentrent d'avantage sur leur développement.

(1) *http://www.kpmg.com/FR/fr/IssuesAndInsights/ArticlesPublications/Documents/the-cloud-takes-shape.pdf*

(2) *« A break in the clouds: Towards a cloud definition », Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres et Maik Lindner*

(3) *http://www.microsoft.com/en-us/news/press/2012/mar12/03-28SMBCloudPR.aspx*

5.12 Article: Data scientist, métier d'avenir ou simple « buzz marketing »?

Data scientist, métier d'avenir ou simple « buzz marketing »?

Par Saïd El Ouazzani

Par sur HBR France :

http://www.hbrfrance.fr/chroniques-experts/2015/06/7397-data-scientist-un-nouveau-metier-en-plein-essor/

Le «*data scientist*» (ou scientifique de données en français) est un métier récent qui est apparu ces dernières années dans le sillage du « big data ». De nombreux débats ont lieu sur sa définition, ses compétences, sa différence par rapport à un statisticien ou un analyste mais également par rapport à la place q'il peut occuper au sein des organisations. Certains spécialistes le voient comme un buzz marketing passager d'autres; au contraire; y voient un nouveau métier d'avenir qui émerge.

Le terme de «*data scientist*» s'est fait connaitre en 2012 après la publication dans HBR de l'article « *Data scientist : The sexiest job of 21st century* »(1). Et depuis, ce métier a gagné de l'importance et est devenu indispensable pour l'analyse et l'exploitation des données au sein des grandes organisations. Cependant, les compétences nécessaires d'un tel profile sont rares et exceptionnelles comme ce fut le cas, à une époque, pour les analystes financiers. Le métier de «*data scientist*» est donc né dans un contexte d'évolution des technologies innovantes comme le «big data». Il doit savoir en tirer profit et faire preuve d'une combinaison des compétences diverses en maitrisant à la fois des concepts statistiques avancées, une culture technique et une compréhension solide des enjeux métiers de son entreprise.

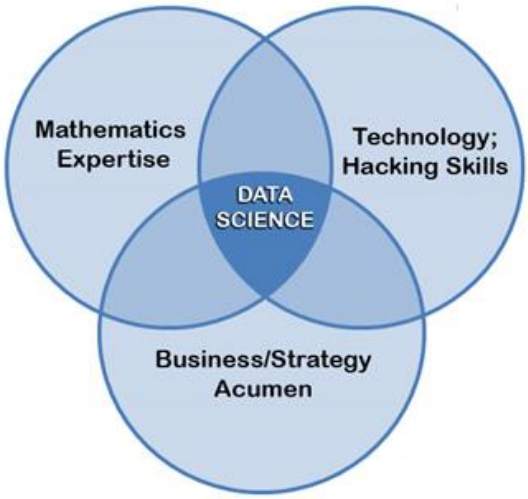


Schéma illustrant les compétences d'un «data scientist»

Comme l'illustre le schéma précédent, les compétences d'un «*data scientist*» s'organisent autour de trois disciplines principales:

- Mathématiques : Le «*data scientist*» a besoin des connaissances en mathématiques, en statistique, et en algorithme. Ces connaissances lui permettent de comprendre des concepts comme le calcul de probabilités, le niveau de signification, etc ;
- Technologique : Le «*data scientist*» est amené à utiliser une panoplie de nouveaux outils techniques de «big data» comme Hadoop, NoSLQ, Mapreduce, Spark, Hive, etc. Son travail au quotidien pour implémenter ses différentes modèles mathématiques nécessite une compréhension des notions informatiques comme le «*clustering*» ou le «*scalling*», etc ;
- Métier : Le «*data scientist*» doit comprendre le métier de son entreprise afin d'analyser les enjeux et maitriser sa stratégie. Cette compréhension lui permet de proposer des nouveaux services et produits à base de données analysées ;

A partir de ces trois dimensions, le spécialiste américain Thomas Davenport («*Big data Strategy» - 2014 – p.92*) liste les différentes compétences nécessaires pour un «*data scientist*»:

- Compétences d'un informaticien:
  - Capacité à coder ;
  - Compréhension des capacités technologiques du «big data» ;
- Compétences d'un consultant:
  - Prise de décision sur la base d'indices ;
  - Fortes compétences en communication et en relationnel ;
  - Capacités à encadrer des décisions et à comprendre les procédures associées ;

- Compétences d'un analyste quantitatif :
  - Analyse statistique et graphique ;
  - Analyse des données structurées et non structurées ;
- Compétences d'un expert commercial :
  - Connaissance du métier ;
  - Capacité à proposer des nouveaux produits à base des données ;

Le profil de «*data scientist*» se démarque des profils de développeur, d'analyste ou de statisticien par sa polyvalence et de l'étendue de son champs d'action. Il combine de compétences très variées et est amené à manipuler des outils «big data» pour développer des nouveaux produits («data products») et services.

---

(1) https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century

5.13 Article : La souveraineté à l'ère du Cloud Computing

La souveraineté à l'ère du Cloud Computing

Non publié – en cours de finalisation – revue Tic&Société

1- Introduction

Nous assistons depuis quelques années à une transformation numérique touchant tous les secteurs d'activités. Cette transformation s'opère dans un monde connecté par l'Internet. Ce dernier est devenu indispensable et vital au même titre que l'eau et l'électricité. Son accès est nécessaire pour l'exercice d'activités et de droits fondamentaux. La complexité des architectures techniques d'Internet et la criticité de ses réseaux supposent une gestion impartiale entre les grandes puissances économiques à l'ère d'émergence de nouveaux modèles technologiques de type Cloud Computing ou BigData.

Conscients des enjeux stratégiques que représentent ces technologies, plusieurs pays appellent à une réforme profonde de la gouvernance de l'Internet. En effet, lors de la 49éme réunion de l'Internet Corporation for Assigned Names and Numbers(1) (ICANN), plusieurs pays membres ont exprimé leurs souhaits de réformer la gouvernance actuelle de l'Internet mondial géré principalement par le département du commerce extérieur des Etats-Unis. Le Brésil, pays faisant parti des BRICS, a accueilli le Net Mundial(2), forum international autour de la gouvernance de l'Internet. L'objectif de cette rencontre internationale est de rendre l'ICANN une organisation indépendante. La Chine, également un des pays de BRICS, a développé un protocole réseau nommé IPv9 compatible IPv6 utilisé actuellement par les réseaux mondiaux. Ce réseau permet au pouvoir central chinois d'isoler son réseau intranet et de se connecter en même temps au réseau mondial d'Internet. Le 11 juillet 2014, Ma Ding, directrice de l'Institut chinois de sécurité de l'Internet à l'Université de la sécurité publique du peuple, a affirmé que les téléphones Apple menaçaient la sécurité nationale. Elle explique que la géolocalisation de millions d'utilisateurs d'iPhone permettait de recueillir des données très sensibles sur les conditions de vie ou l'économie d'un pays, voire des secrets d'État. Ces multiples exemples confirment les enjeux stratégiques liés à ces technologies innovantes, ainsi que cette course des grandes puissances pour dominer le paysage numérique mondial.

À l'heure de la mondialisation, plusieurs questions se posent : Qui gère l'infrastructure numérique mondiale ? Quels sont les acteurs de Cloud Computing ? Quels sont les enjeux économiques, techniques et juridiques qui y sont liés ? Les Etats sont-ils toujours souverains à l'ère du Cloud Computing et du tout numérique?

2- De l'Internet au Cloud Computing :

A travers l'histoire récent du numérique, il y a eu une succession de batailles technologiques. Au départ, ce fut autour des microprocesseurs puis des systèmes d'exploitation (OS) suivi par les télécoms dont les européens ont résisté jusqu'à l'arrivée des téléphones intelligents (smartphones) à l'image du déclin du français Alcatel-Lucent et du finlandais Nokia. Les prochaines batailles à venir se porteront principalement autour des technologies innovantes dont le Cloud Computing.

Le terme Cloud Computing ou l'« Informatique dans les nuages » vient du monde des télécoms. Il permet de représenter les réseaux des télécommunications et symbolise le traitement de l'information d'une manière transparente à l'utilisateur. **Exemple**: Un utilisateur envoie une requête sur un siteweb, il reçoit un résultat en retour sans savoir exactement où l'information a été stockée ni d'où elle provient ni comment elle a été traitée.

Il existe plusieurs définitions de Cloud Computing, l'article paru en 2008 « *A break in the clouds: Towards a cloud definition* »[3] en recense 22 définitions. La définition la plus répandue est celle du National Institute of Standards and Technology (NIST), une agence du département du commerce des États-Unis, qui définit le Cloud Computing comme étant : *« l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées et configurables* »[4]**.** En France, la Commission générale de terminologie et de néologie, dont la mission est de favoriser l'enrichissement de la langue française, défini le Cloud Computing comme étant un « *Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire*». Cette définition a apparu dans le journal officiel n°0129 du 6 juin 2010. La définition du Cloud Computing se résume donc aux principes suivants :

- Une consommation des services à travers des technologies web : La messagerie électronique (Gmail, Hotmail, Yahoo mail, …) par exemple.
- Une gestion du logiciel ou du matériel abstraite d'un point de vue client. Ce dernier se concentre sur son cœur de métier et sous-traite cette gestion à des prestataires spécialisés.
- Un accès libre via Internet aux ressources informatiques depuis n'importe où et à tout moment avec un paiement flexible selon la consumation.

Techniquement, le Cloud Computing s'appuie sur des infrastructures matérielles (des centres de données hébergeant des applications informatiques) reliées entre-elles par des réseaux de la fibre optique. Cette dernière a un statut juridique très hétérogène dû à la multiplicité des acteurs privés et publics. Ainsi dans une économie numérique où 89% du trafic Internet mondial passe par la fibre optique, ces installations techniques constituant le cœur du Cloud Computing sont considérées stratégiques mais également commerciales. Les grands acteurs du Cloud Computing, dont la majorité est en relation avec les Etats-Unis, tirent la grande partie de la valeur générée par ce trafic sans pour autant participer au développement de ces infrastructures numériques financées principalement par des fonds publics. Par conséquent, des règles de gestion doivent être définies entre les opérateurs

télécoms, les acteurs du Cloud Computing et les pouvoirs publics afin de partager équitablement la valeur générée par cette nouvelle économie numérique et pouvoir rembourser les fonds investis. **Exemple** : L'opérateur télécom français Free a bloqué l'accès à YouTube (Une plateforme Cloud de partage des vidéos appartenant à l'américain Google) au lancement de son offre Free Box Révolution. L'objectif était de protéger la bande passante Internet de Free contre l'accès excessif des clients aux vidéos hébergés par YouTube. Google tire les bénéfices à travers la publicité et le nombre des clients tout en dégradant la qualité de service de Free.

3- De la souveraineté à la souveraineté numérique :

Le concept de la souveraineté a été introduit pour la première fois par Jean Bodin qui est considéré comme le fondateur théorique de l'idée de l'État souverain. Dans son œuvre sur la République écrite en 1576, il précise les principes et les caractéristiques de la souveraineté et du bon fonctionnement de l'État. Par la suite en 1896, dans L'«*'État fédéral et confédération d'états*»[(5)], Louis Le Four en donne la définition suivante : « *La souveraineté est la qualité de l'État de n'être obligé ou déterminé que par sa propre volonté, dans les limites du principe supérieur du droit, et conformément au but collectif qu'il est appelé à réaliser* ». Dans la constitution française de 1958, la notion de la souveraineté est définie dans les articles suivants:

- **Article 2**[(6)] qui définit les principaux symboles de la république et le principe de gouvernement de la République française.
- **Article 3**[(7)] qui fait partie du titre I sur la souveraineté, et traite de l'exercice de la souveraineté nationale.
- **Article 4**[(8)] qui traite les rôles des partis et groupements politiques et du principe de démocratie.

La souveraineté consiste à concentrer le pouvoir et la force dans l'Etat pour défendre son indépendance à l'extérieur comme à l'intérieur. C'est une expression collective des choix des citoyens sans subordination à une autorité étrangère. Les seules limitations de ces choix proviennent du droit international et des traités dont les traités européens.

Le terme souveraineté au niveau européen renvoie à une forme de protectionnisme incitant les politiques à préconiser le développement d'une protection économique européenne face aux pays émergents[(9)]. L'Union européenne est une communauté constituée par des unités politiques, des États souverains qui la composent. A l'intérieur de l'Union, la souveraineté signifie que les États-membres transfèrent certains droits de décision aux institutions qu'ils ont mis en place.

La souveraineté numérique, quant à elle, consiste à appliquer les principes de la souveraineté au domaine numérique pour assurer la sécurité des installations technologiques stratégiques et protéger les échanges des données sensibles et confidentielles de l'Etat et des citoyens.

En France, dans un article des Echos apparu en 2011[(10)], le président de la radio SkyRock, Pierre Bellenger, définit pour la première fois la souveraineté numérique comme étant *«la*

maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques». Et suite à une consultation publique lancée par le Conseil national du numérique[(11)] la même année, Pierre Bellenger indiquait dans sa note: «*Il n'y'a pas de souveraineté nationale sans souveraineté numérique. L'Internet est un réseau mondial sous contrôle des États-Unis. Les entreprises américaines y sont le plus souvent dominantes. La dépendance et le transfert de valeur occasionnés par ce déséquilibre doivent amener les pouvoirs publics à mettre en œuvre une politique industrielle de l'Internet*». Conscient des enjeux liés au numérique, dans une interview accordée le 28 novembre 2012 à L'Express sur la politique gouvernementale relative aux nouvelles technologies, la ministre française déléguée à l'Économique numérique indiquait vouloir «*défendre notre souveraineté numérique*».

4- La souveraineté à l'air de Cloud Computing :

La gestion de l'Etat moderne n'est pas différente de la gestion d'une entreprise privée innovante. L'Etat et ses administrations doivent se configurer autour des services innovants pour répondre aux aspirations quotidiennes des citoyens. Au cœur de cette innovation, toutes les technologies autour du Cloud Computing. Cet Etat, moderne et souverain, doit être sous contrôle des citoyens. Il est le garant de leurs droits et libertés individuelles. La France, cinquième puissance économique mondiale, fait partie des premiers exportateurs mondiaux des données à caractère personnel (*selon l'Art. 2 de la loi «Informatique et libertés»[(12)], sont considérées comme données à caractère personnel : Adresse IP, nom, n° d'immatriculation, n° de téléphone, photographie, …)*. Ces données sont stockées sur des serveurs Cloud Computing américains et répondent de la compétence de juridictions américaines. Or dans un article de Patrick Baillie[(13)], CEO de CloudSigma (fournisseur des solutions Cloud Computing américain), affirme qu'indépendamment de la localisation physique des centres de données (datacenters), celles-ci seront in fine soumises au Patriot Act**,** si le centre de données appartient et est géré par un acteur américain, y compris si c'est en violation de la législation française ou européenne. Pour rappel, le Patriot Act[(14)] est une la loi votée par le Congrès américain le 26 octobre 2001 afin de renforcer les pouvoirs des agences gouvernementales dans la lutte contre le terrorisme. Cet enjeu de vie privée mais aussi de compétitivité économique et de sécurité nationale constitue un véritable transfert de souveraineté de la France – numérique soit-elle- vers une autorité étrangère. Selon les principes fondamentaux de la souveraineté – comme décrit plus haut - le rôle d'un Etat souverain est d'assurer la protection des données sensibles, la sécurité de ses citoyens et de veiller aux respects des lois en vigueur. D'ailleurs, pour certains pays, seulement quelques points concentrent l'accès à toutes les communications (télécom, Internet, …) et créent ainsi une fragilité aux attaques ou aux censures de tous types.

La protection des données sensibles et des installations technologiques critiques doivent bénéficier des mêmes surveillances que les réseaux ferroviaires, électrique ou aériens pour faire face à tout acte criminel, terroriste voire acte de guerre. La sécurité intérieure dépend principalement de l'intégrité des infrastructures informatiques et des équipements réseaux

utilisés qui constituent une partie intégrante du système de défense national Français. Le rapport d'information sénatorial n° 681 (2011-2012) de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012[(15)], pointe du doigt les liens entre les industriels chinois ZTE et Huawei (dont l'Etat Chinois est actionnaire) et le pouvoir central chinois. Ce rapport liste dix priorités stratégiques pour la France et préconise quarante recommandations. L'une des priorités listées par ce rapport, la dixième, propose « *d'interdire sur le territoire national et à l'échelle européenne le déploiement et l'utilisation de routeurs ou d'autres équipements de cœur de réseaux qui présentent un risque pour la sécurité nationale, en particulier les routeurs et certains équipements d'origine chinoise*». Sur le plan chronologique, le concept de sécurité nationale ait été employé dans le cadre des télécommunications en 1991. Selon l'article 3 du texte de 1991, il est cité : *«peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des télécommunications ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées*». Cet article a été réactualisé en 2013. Dans le même sens, le président de la république, dans un discours prononcé en 2007, a déclaré : *« De ce travail émerge un nouveau concept ; celui d'une stratégie de sécurité nationale qui associe, /…/, la politique de défense, la politique de sécurité intérieure, la politique étrangère et la politique économique. Cette stratégie porte une ambition européenne et internationale qui est au cœur de la vocation de la France dans le monde*». Aux États-Unis, un rapport du Congrès[(17)] préconise également le bannissement des équipements télécoms chinois appartenant aux entreprises Huawei et ZTE. Malgré ces soupçons d'espionnage, dans un article diffusé par l'Agence France Presse (AFP)[(16)], le gouvernement français vient de signer un plan stratégique d'investissement de 3,3 milliards d'Euros avec le géant chinois Huawei pour développer ses activités dans l'Hexagone**.**

Le 5 Juin 2013, les deux journaux the Washington Post et The Guardian ont publié une note secrète sous le code s.125 du Patriot Act incitant l'opérateur Télécom américain Verizon à fournir à la NSA (National Security Agency) les détails des appels téléphoniques de tous les citoyens américains. Le 6 Juin 2013, les deux journaux ont révélé l'existence d'un vaste programme de surveillance de la NSA nommé PRISM permettant l'accès aux données hébergées par les grandes entreprises américaines du web: Google, Amazon, Microsoft, … . Ces mêmes entreprises sont également les principaux fournisseurs des solutions Cloud Computing dans le monde. Dans la même journée, le directeur de la NSA, ADAM Clapper, a reconnu officiellement l'existence de ce programme en précisant qu'il est lié au FISA Amendment 2008 s.1881a/702 (FAA)[(18)]. Le 09 Juin 2013, Edward Snowden, ex-consultant de la NSA, a volontairement révélé les différents détails de ce vaste programme d'espionnage. L'Union Européenne dans sa résolution de 04 Juillet 2013 concernant ce programme de surveillance de la NSA a fermement condamné l'espionnage de ses représentations

officielles et a demandé aux autorités américaines de fournir toutes les informations nécessaires à la compréhension de ce programme.

Malgré cette inquiétude européenne, le programme PRISM mené par la NSA s'inscrit dans la continuité des programmes de surveillance américains depuis la deuxième guerre mondiale. Les outils exploités par les autorités américaines illustrent la puissance numérique de ce pays et la difficulté des autres pays (compris les pays de l'Union Européenne) à se protéger contre ces programmes d'espionnage. En parallèle du programme PRISM, la NSA contrôle et surveille toutes les communications internationales via un autre programme appelé : «Upstream». En effet, avec «Upstream », la NSA surveille toute l'infrastructure réseaux et intercepte tout le trafic passant par les fibres optiques transatlantiques et rapatrie les informations collectées vers des centres de décision au Fort Meade près de Washington ou des centres de calcul à Bluffdale ou celui d'Utah, selon un article de Libération apparu le 27 juin 2013, ce dernier centre est capable d'héberger 5000 milliards de Giga octets. La répartition mondiale de ces puissances de calcul éclaire les capacités de chaque pays en matière de défense, de recherche et de contrôle.

En 1963, Allen Dulles avait déclaré : «*Notre gouvernement, dans sa nature même, et notre société ouverte dans toute son instinct, en vertu de la Constitution et la Déclaration des droits de l'homme, interdit automatiquement les services de renseignement se sont développées dans des États policiers* »[(19)]**.** En 2013, Eric Schmidt, le PDG de Google, a déclaré de son côté que « *Il y'a eu d'espionnage pendant des années, il y'a eu de la surveillance pendant des années, et ainsi de suite, sans porter des jugements, c'est la nature de notre société*»[(20)]**.**

Certes les deux déclarations ont 50 ans d'écart mais elles renvoient vers cette question centrale de savoir comment les démocraties peuvent continuer d'exister dans leurs formes actuelles si ces programmes de surveillances continuent de fonctionner et si les pays transfèrent leurs souverainetés à des grandes entreprises supranationales. Pour Eric Schmidt, les différents rapports mondiaux sont clairs, le monde a changé et «*il n'est plus possible de nager contre le courant* ».

5- Vers une politique industrielle souveraine :

Pour assurer sa souveraineté numérique, faire face à l'espionnage chinois et mettre terme au transfert massif des données vers les serveurs américains, beaucoup d'observateurs et experts considèrent qu'une prise de conscience des pouvoirs publics est nécessaire. Cette prise de conscience permet d'établir une politique industrielle souveraine en matière des nouvelles technologies et développer des alternatives numériques nationales.

Aux Etats-Unis, il existe une vraie politique numérique souveraine. L'univers numérique américain bénéficie d'un support public et de plusieurs partenariats public-privé (PPP). A titre d'exemple, on peut citer le rôle de de US Darpa (Defense Advance Research Project Agency) dans le domaine de la défense nationale américain.

Après le « Plan calcul »[21], le plan gouvernemental français lancé en 1966 par le général De Gaulle destiné à assurer l'indépendance du pays en matière de gros ordinateurs, le « Plan informatique pour tous »[22], le programme du gouvernement qui devait permettre d'initier les 11 millions d'élèves du pays à l'outil informatique et de soutenir l'industrie nationale, le « Plan câble »[23], mis en place par les lois du 29 juillet 1982 et du 1er août 1984 et qui prévoyait le câblage en 10 ans de 52 de principales villes de France, le « Plan national très haut débit »[24], qui vise à couvrir l'intégrale du territoire en très haut débit d'ici à 2022. Il est temps pour l'Etat français de lancer le «Plan Cloud Computing». Ce nouveau plan consiste à construire un Cloud Computing purement français qui constitue une alternative aux solutions Cloud Computing étrangères. C'est ainsi que viennent d'être portés sur les fonds publics deux grands projets avec un coût de 150 millions d'euros via la caisse des dépôts dans le cadre de la politique des fonds d'investissements[25] de l'Etat. Une somme qui bénéficiera à deux consortiums : Cloudwatt[26] porté par Orange et Thalès et Numergy[27] porté par SFR et Bull. A ce paysage s'ajoute des jeunes entreprises numériques innovantes dans le Cloud Computing que l'Etat doit soutenir dans le cadre de cette politique industrielle. En effet, et depuis plusieurs années, ces entreprises françaises de forte croissance, qui ont grandi sans subvention ni soutien public, parmi lesquelles OVH, Ikoula, Gandi ou Néo Télécoms, se sont positionnées et sont aujourd'hui reconnues sur ce marché à l'échelle européenne voir mondiale. Dans l'optique de créer un « Cloud souverain français » et un « championnat européen », le rôle de l'Etat serait de fédérer tous ces acteurs spécialisés, apportant leur savoir-faire et leur technologie, au sein d'un consortium aux côtés de grands acteurs et de laboratoires de recherche nationaux.

Pour rendre la France une nation millénaire capable de reconfigurer son fonctionnement et son économie autour du numérique et par conséquent, assurer sa souveraineté et sa souveraineté numérique, l'État doit rassembler tous les acteurs autour d'un vrai projet national, à la fois complet, innovant, pérenne et au service des administrations publiques, des entreprises et des citoyens.

6- Conclusion

Le principe de liberté des mers, issu du 17^{éme} siècle, ne fut que l'incarnation d'une domination anglo-saxonne des océans. L'Internet est semblable à l'océan. Comme lui, Il est un lien universel entre tous les territoires. La domination anglaise des mers à l'ère d'Elizabeth 1er a changé l'histoire. Lui a succédé la domination sous-marine américaine au 20^{éme} siècle. Par transposition, en remplaçant le maritime par Internet, ce dernier est universel et relie tous les territoires sans en être un, il oppose son caractère planétaire aux souverainetés qui se définissent dans des espaces physiques délimités. Comme ce fut le cas des océans avec la reine Élizabeth 1er, celui qui contrôle les codes du numérique, espère gouverner le monde de demain.

7- Références bibliographiques:

(1) https://www.icann.org/

(2) http://www.01net.com/editorial/618468/netmundial-la-gouvernance-dinternet-se-cherche-dans-un-climat-de-defiance/

(3) https://www.research.ibm.com/haifa/projects/systech/reservoir/public/CloudDefinitionPaper.pdf

(4) http://www.nist.gov/index.html

(5) État fédéral et confédération d'états par Louis Le Fur (1896) p. 443

(6) http://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000006527453&cidTexte=LEGITEXT000006071194&dateTexte=vig

(7) http://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000019240995&cidTexte=LEGITEXT000006071194&dateTexte=vig

(8) http://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000019240999&cidTexte=LEGITEXT000006071194&dateTexte=vig

(9) Le taux moyen de protection de l'Europe est certes très faible (1,47 %) mais il est identique à celui des États-Unis (1,43 %) et du Japon (1,41 %). Celui de la Chine s'élève à 2,1 %, le Brésil à 6 % et l'Inde à 8 %.

(10) http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

(11) Organisme consultatif français créé le 29 avril 2011 par le Décret no 2011-4761 puis réorganisé par le décret n° 2012-1400 du 13 décembre 2012

(12) http://www.cil.cnrs.fr/CIL/spip.php?rubrique299

(13) http://www.forbes.com/sites/ciocentral/2012/01/02/can-european-firms-legally-use-u-s-clouds-to-store-data/

(14) http://www.e-juristes.org/usa-patriot-act/

(15) http://www.senat.fr/rap/r11-681/r11-681_mono.html

(16) http://www.challenges.fr/high-tech/20140930.CHA8291/telecoms-huawei-veut-investir-1-5-milliard-d-euros-en-france.html

(17) http://www.zdnet.fr/actualites/un-rapport-du-congres-americain-preconise-le-bannissement-des-equipements-telecoms-chinois-39783330.htm

(18) http://fr.wikipedia.org/wiki/FISA_Amendments_Act_of_2008

(19) Dulles, Allen Welsh (1963), The Craft of Intelligence, New York: Harper&Row, p.257. « Our government in its very nature, and our open society in all its instinct, under the Constitution and the Bill of Rights automatically outlaws intelligence organizations of the kind that have developed in police states »

(20) http://www.theguardian.com/world/2013/sep/13/eric-schmidt-google-nsa-surveillance : « There's been spying for years, there's been surveillance for years, and so forth, I'm not going to pass judgment on that, it's the nature of our society»

(21) http://fr.wikipedia.org/wiki/Plan_Calcul

(22) http://fr.wikipedia.org/wiki/Plan_informatique_pour_tous

(23) http://www.arcep.fr/uploads/tx_gspublication/rapport-conv-cable-juillet2007.pdf

(24) http://www.lesnumeriques.com/france-tres-haut-debit-carte-debits-est-en-ligne-n35228.html

(25) http://www.journaldunet.com/solutions/cloud-computing/comparatif-cloudwatt-numergy-clouds-souverains/

(26) https://www.cloudwatt.com/fr/

(27) https://www.numergy.com/fr/

(28) http://www.amazon.com/Land-Meer-Carl-Schmitt/dp/3608941975

5.14 Article : Quel rôle pour la DSI à l'ère du cloud. Centre de profit ou centre de coût ?

Quel rôle pour la DSI à l'ère du cloud : Centre de profit ou centre de coût ?

Publié sur HBR :

http://www.hbrfrance.fr/chroniques-experts/2016/04/10721-et-si-votre-service-informatique-vous-faisait-gagner-de-largent/

Il y a 150 ans, le célèbre photographe Français Félix Tournachon avait défini les 3 éléments de la modernité suivants: « Photographie, Electricité et Aéronautique». S'il est parmi nous aujourd'hui, il aurait certainement ajouté un quatrième élément: « Internet ». Ce constat est confirmé par le rapport Accenture Technology Vision 2015 – « Internet of Me » Trend (1).

Comme l'explique l'universitaire Imed Boughzala dans cet article (2) d'Harvard Business Review, avec le passage des organisations d'un modèle 2.0 vers un modèle plus intelligent, dit 3.0, le rôle joué par les directions des systèmes d'informations (DSI) au sein des organisations est en constante transformation avec l'arrivée de Cloud Computing, Bigdata, Green IT, Internet of Things, … .

Cette évolution technologique, mais aussi stratégique, offre aux DSI de nouvelles opportunités de développement. En effet, selon une étude de Gartner, en 2020, les dépenses opérationnelles seront divisées par deux et celles consacrées à l'innovation seront triplé. Cette réduction de coûts et de dépenses s'explique par l'adoption des nouveaux *Business Models* orientés service. Selon le Gartner 2015 CIO Agenda Survey, le cloud figure parmi les 3 investissements prioritaires des DSI pour les années à venir.

Rank	Investment priority	2014	2015
1	BI/analytics	41%	50%
2	Infrastructure and data center	31%	37%
3	Cloud	27%	32%
4	ERP	26%	34%
5	Moblie	24%	36%
6	Digitalization/digital marketing	17%	11%
7	Security	13%	11%
8	Networking, voice and data comms	12%	12%
9	Customer relationship/experience	11%	8%
10	Industry-specific applications	9%	10%
11	Legacy modernization	7%	7%
12	Enterprise applications	6%	2%

Comparaison des investissements entre 2014 et 2015 (extrait de l'étude Gartner)

La disponibilité des services dans le cloud et le pay-as-you-go pricing model (paiement à la consommation) incitent les DSI à considérer la technologie autrement et à se concentrer d'avantage sur les besoins métier. Ce changement du rôle d'un simple fournisseur de service informatique vers un rôle de stratège au sein de la direction générale consiste à transformer la DSI d'une structure considérée comme un centre du coût (Cost Center) vers une structure vue comme un centre de profit (Profit Center). Pour différencier ces deux modèles d'organisation, un centre de profit est une structure présentant un résultat d'exploitation avec une colonne « coûts » et une colonne «revenus », alors qu'un centre de coûts fonctionne sur une dotation budgétaire.

Comment transformer la DSI d'un Cost-Center vers un Profit Center :

Selon une étude menée au niveau mondial par Emerson Network Power en 2013 (3), 50% des 560 décideurs IT interrogés considèrent la DSI comme un centre de coût et de dépense pour lequel le Cost-killing (réduction des coûts) est devenu la règle. A l'inverse, d'autres DSI qui font appel à des services Cloud sont considérées, par leurs organisations, comme un centre de profit générant de bénéfice et une valeur ajoutée au métier. Par exemple, selon l'approche Cloud de NIST, une solution SaaS de gestion de clientèle comme salesforce.com est considérée par les départements Marketing comme un service à valeur ajoutée. Ce service permet à ce département de centraliser les informations clients et de consolider l'historique provenant de centre d'appels, des emails et des réseaux sociaux. Cette solution Cloud met également à disposition des outils d'analyse et d'aide à la décision.

Pour rappel, l'approche de National Institute of Standards and Technologies (NIST) consiste à définir le Cloud sous forme de trois couches différentes:

1. Software as a Service (SaaS) qui consiste à ne plus installer les applications sur ses propres serveurs mais de s'abonner à des services disponibles dans le cloud. Salesforce.com est un exemple d'une offre SaaS.

2. Platform as a Service (PaaS) qui permet d'accéder à des applications middleware (Bases de données, Couches d'intégration de données, …) ainsi qu'aux environnements techniques chez un fournisseur Cloud. Google Apps Engine est un exemple d'une offre PaaS.

3. Infrastructure as a Service (IaaS) qui consiste à externaliser l'infrastructure matérielle (serveurs, réseau et stockage) chez un fournisseur Cloud et les faire évoluer à la demande et à distance. L'offre EC2 d'Amazon.com est un exemple d'IaaS.

Dans le contexte d'une DSI, le rôle classique (Cost-Center) consiste à fournir gratuitement des services informatiques au métier. Le budget alloué chaque année permet de couvrir les coûts associés au fonctionnement : achat de matériel, recrutement de

personnels, achat des licences, maintenance des applications, … . A l'inverse, une DSI organisée comme un centre de profit a la capacité de réduire considérablement ses coûts en faisant appel à des services disponibles dans le cloud. Ces services sont par la suite refacturer au métier. Le profit généré par la DSI participe à la croissance globale de l'entreprise.

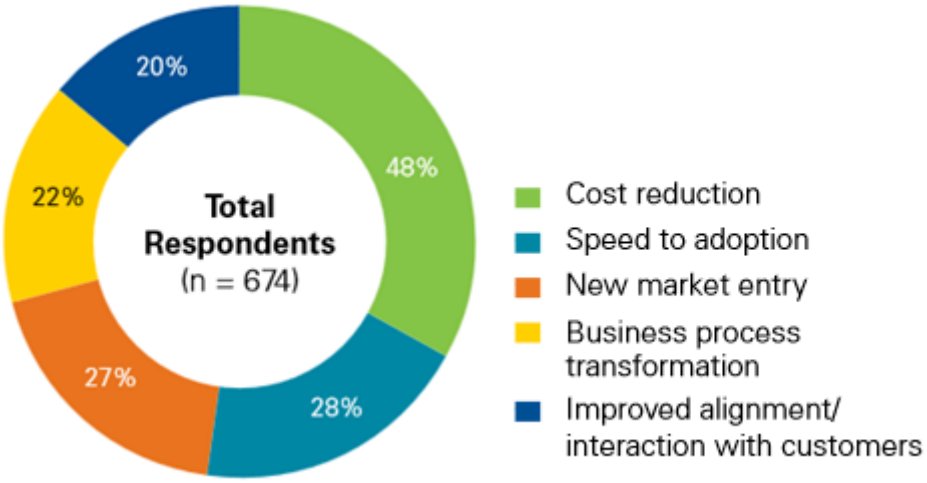
Comment générer du profit avec les services Cloud:

L'étude de cas illustré dans cet article montre qu'une entreprise pourrait réduire considérablement ces coûts informatiques selon les axes suivants :

1. Louer les services au lieu d'acheter des solutions informatiques propres. Cela permet à l'entreprise de transformer le capital en dépenses opérationnelles variables en capital d'investissement (Opex, par opposition au Capex).

2. Se décharger de la gestion : Les fournisseurs Cloud sont les responsables des services fournis : mise en place, configuration, maintenance, etc.

3. Améliorer la stratégie «Go-to-Market» : Les services Cloud permettent aux entreprises de gagner en flexibilité, en rapidité de mise en place.



Objectifs visés de la migration vers le cloud (extrait de l'étude KPMG)

(1) http://www.hbrfrance.fr/chroniques-experts/2014/11/5243-comment-la-transformation-du-systeme-dinformation-impacte-lorganisation/
(2) http://www.emersonnetworkpower.com/en-EMEA/Solutions/CIO-Topics/Documents/CIO-of-the-Future-Research-Report_fr.pdf
(3) http://techtrends.accenture.com/us-en/internet-of-me.html
(4) http://www.kpmg.com/FR/fr/IssuesAndInsights/ArticlesPublications/Documents/the-cloud-takes-shape.pdf

Résumé

Titre : Analyse des politiques publiques en matière d'adoption du Cloud Computing et du Big data. Une Approche comparative des modèles français et marocain.

Mots clés : Cloud Computing, Big data, Cyber-État, politique publique, numérique, sécurité.

Résumé:

Notre recherche consiste en l'analyse des politiques publiques françaises et marocaines en matière d'adoption des technologies du Cloud Computing et du Big data. A travers ce travail, nous avons analysé ce que les deux États - français et marocain - font (ou ne font pas) pour faire face aux enjeux du numérique. Des enjeux pour lesquels l'État d'aujourd'hui doit apporter une réponse politique et technique. En effet, selon sa conception wébérienne, l'État se voit se transformer vers une nouvelle représentation dans le cyberespace sous forme d'un Cyber-État. Ce dernier aura pour mission:

- Assurer une souveraineté de l'État en développant des plateformes Cloud Computing nationales capables de fournir les mêmes services que les plateformes Cloud Computing étrangères ;
- Développer des outils technologiques autour du Big data conjugués à des solutions Cloud Computing pour améliorer les services publics. En effet, la donnée est devenue un enjeu commercial et politique. Sa bonne maitrise permettrait à l'État une meilleure élaboration des politiques publiques ;
- Développer une présence de l'État et l'ensemble de ses administrations sur le cyberspace. Ainsi, les citoyens, ou les cyber-citoyens, puissent interagir avec l'État, contrôler son fonctionnement et ainsi promouvoir une démocratie participative de proximité ;
- Mettre en place des outils Cloud Computing et Big data au service de la sécurité nationale pour faire face aux programmes d'espionnages étrangers. Cependant, ces outils ne doivent pas servir à la convergence d'un État du contrôle et de la surveillance.

Dans un contexte de transformation profonde de la société provoquée par le numérique, l'État doit ré affirmer son droit sur son territoire. En effet, l'Internet offre aux individus des possibilités de sociabilité croissantes à travers une «vie numérique» qui constitue le prolongement de la vie réelle. Cette vie numérique des individus évolue en parallèle de l'évolution de la technologie qui fait accélérer la sociabilité en ligne. Cette sociabilité s'accompagne avec des contraintes liées au traitement des données personnelles et fait surgir des débats autour de la vie privée.

Pour faire face aux risques sécuritaires, la France, comme le Maroc, se sont dotés des instruments juridiques et techniques qui s'appuient sur les technologies du Cloud Computing et du Big data. L'arsenal juridique français s'est vu renforcé dernièrement par l'adoption successive (et accélérée

sans débat national) de la loi de programmation militaire (2014-2019) puis de la loi anti-terroriste (adoptée en 2014) et dernièrement de la loi sur le renseignement (adoptée en 2015). Ces différents textes ont agité le débat politique par une inquiétude grandissante autour du déploiement de dispositifs numériques de surveillance. Une surveillance, ou une cybersurveillance, qui se légitime par la lutte contre le terrorisme en faisant, chaque fois que nécessaire, référence à la notion de la sécurité nationale. Cette dernière considérée comme restrictive des libertés publiques et individuelles. Son contenu n'est pas défini, et est donc flou et reste à la discrétion des autorités publiques.

A travers ce travail, nous avons donc couvert quatre axes principaux :

1. L'évolution de l'État vers le modèle du Cyber-État. Une évolution qui implique la mise en place des cyber-politiques publiques associées ainsi que le développement du cyber-secteur public, du cyber-service public et également une évolution de la fonction publique.

2. Les enjeux sécuritaires à l'ère du Cyber-État. En effet, nous avons traité les notions de la cybersécurité, la cybersouveraineté et la cybersurveillance au sein du Cyber-État. Nous avons analysé également le développement de la notion de la « sécurité nationale » comme doctrine d'État et précisément avec l'adoption de différentes lois liées à la sécurité nationale : loi de programmation militaire, loi anti-terroriste, loi relative sur le renseignement.

3. Les enjeux liés au traitement des données personnelles au sein du Cyber-État. En effet, nous avons analysé les enjeux autour de la donnée. Une donnée produite à travers les activités quotidiennes du cyber-citoyen (ou le citoyen connecté).

4. Les fondements techniques du Cyber-État : Cloud Computing et Big data. Nous avons essayé de proposer une approche technique et fonctionnelle des deux technologies et analyser les différents enjeux associés.

A la fin et en collaboration avec des partenaires français (Mairie de Boulogne-Billancourt) et américains (Engaged Public et CausesLabs) nous avons pu montrer à travers une étude de cas l'apport concret du Cloud Computing pour une collectivité locale française. Une expérimentation qu'elle conviendrait de continuer à développer dans l'avenir.

Thesis title : Public Policies Analysis for Cloud Computing and Big data adoption. Comparative Approach between French and Morrocan Models.

Key words : Cloud Computing, Big data, Public Policy, Digital, Security, Internet, Governance

Abstract:

Our research concerns the public policy analysis on how Cloud Computing and Big data are adopted by French and Moroccan States with a comparative approach between the two models.

We have covered these main areas:

- The impact of the digital on the organization of States and Government ;
- The digital Public Policy in both France and Morocco countries ;
- The concept related to the data protection, data privacy ;
- The limits between security, in particular home security, and the civil liberties ;
- The future and the governance of the Internet ;
- A use case on how the Cloud could change the daily work of a public administration ;

Our research aims to analyze how the public sector could be impacted by the current digital (re) evolution and how the States could be changed by emerging a new model in digital area called Cyber-State. This term is a new concept and is a new representation of the State in the cyberspace.

We tried to analyze the digital transformation by looking on how the public authorities treat the new economics, security and social issues and challenges based on the Cloud Computing and Big Data as the key elements on the digital transformation. We tried also to understand how the States – France and Morocco - face the new security challenges and how they fight against the terrorism, in particular, in the cyberspace. We studied the recent adoption of new laws and legislation that aim to regulate the digital activities. We analyzed the limits between security risks and civil liberties in context of terrorism attacks. We analyzed the concepts related to the data privacy and the data protection.

Finally, we focused also on the future of the internet and the impacts on the as is internet architecture and the challenges to keep it free and available as is the case today.

Fin.

Dernière mise à jour, Samedi 28/08/2016 à 01h40