Les Émirats arabes unis et la révolution numérique : nouveaux défis pour le droit public, le droit privé et le droit pénal

Musabbeh Alsaedi

UNIVERSITÉ PARIS I PANTHÉON SORBONNE

UFR de droit des affaires

Laboratoire de rattachement : Institut de recherche juridique de la Sorbonne

THÈSE

Pour l'obtention du titre de Docteur en Droit

Présentée et soutenue publiquement

Le 05/07/2022 par

M. Musabbeh ALSAEDI

LES EMIRATS ARABES UNIS ET LA RÉVOLUTION NUMÉRIQUE. NOUVEAUX DEFIS POUR LE DROIT PUBLIC, LE DROIT PRIVÉ ET LE DROIT PÉNAL. Sous la direction de Monsieur le Professeur Philippe Delebecque.

Professeur des universités [Droit privé et sciences criminelles] à l'Ecole de droit de la Sorbonne (Université Paris 1 Panthéon-Sorbonne)

Membres du Jury

Monsieur le Professeur Marius TCHENDJOU, MCF, Droit privé et sciences criminelles à l'Université de Reims « Rapporteur ».
Monsieur le Professeur Mostefa MAOUENE, professeur à l'Université de Sidi Bel Abbès « Rapporteur » .
Monsieur le Professeur Jean-Denis PELLIER, Professeur de droit privé et sciences criminelles à l'Université de Rouen .

Remerciements

Il me sera très difficile de limiter mes remerciements à une simple page, car c'est grâce à de nombreuses personnes que j'ai pu mener à bien ces travaux de recherche.

Je tiens à remercier grandement mon directeur de thèse Monsieur le Professeur Philippe DELEBECQUE, d'avoir accepté de diriger ce projet de recherche, pour tous ses conseils , son aide et ses remarques à la fois productives et bienveillantes au cours de l'élaboration de ce travail.

Je remercie également Monsieur le Professeur Mostefa MAOUENE, Professeur de droit privé et de sciences criminelles à la faculté de droit et des sciences politiques à l'université Djilali Liabès-Sidi bel Abbès, ainsi qu'au Monsieur le Professeur Marius TCHENDJOU, MCF à l'Université de Reims, qui m'ont fait l'honneur d'accepter de participer à mon jury de thèse et d'être les rapporteurs de cette thèse. Ainsi, qu'au Monsieur le professeur Jean-Denis PELLIER, Professeur de droit privé et sciences criminelles à l'Université de Rouen, pour l'honneur qu'il m'a fait qui m'a fait l'honneur d'accepter de participer à mon jury de thèse.

Je remercie infiniment mes parents, ma famille et à tous mes amis qui m'ont soutenu, supporté et encouragé tout au long de ce périple de recherche.

Résumé

La thèse entend évoquer toutes les implications de la révolution numérique aux Emirats Arabes Unis, dans une perspective juridique. En regard de l'actualité, un accent particulier est porté sur la menace de la cybercriminalité. Comment la conjurer alors que les techniques d'agression ne cessent de se perfectionner au fil des années ?

D'une part, dans notre thèse, je tente de dresser un panorama de l'existant, à savoir l'histoire et la situation particulière des Emirats, sans oublier le caractère fédéral de sa structure institutionnelle. Il est également indispensable, de façon plus globale, de faire un tour d'horizon, bien entendu toujours à compléter et à changer, des différents aspects, positifs et menaçants de la révolution numérique.

Dans la mesure où le pays étudié en est au début de la mise en place d'une législation en la matière, l'attention est portée à la façon dont d'autres pays, surtout la France et les Etats-Unis, relèvent ces nouveaux défis. Pour tenter d'avancer de façon comparative. Il est évident que la révolution numérique s'incarne différemment selon le pays concerné, et aussi le moment qu'il traverse. Mais la dimension locale renvoie toujours à une dimension globale dans un monde de plus en plus interconnecté. L'hyper-mondialisation, malgré des moments de recul, rend impérative autant que délicate une législation à si vaste échelle.

En amont, une réflexion est menée sur la manière dont le droit peut et doit affronter des enjeux très complexes, des exigences en tension, sinon des dilemmes par exemple entre davantage de sécurité et une liberté intégralement préservée. Dans un contexte en perpétuelle évolution. En aval, la révolution numérique ne consiste pas seulement en des dangers mais permet des progrès incontestables dans le sens de plus de participation démocratique, plus d'efficacité et de coordination.

En fait, le bilan est nuancé et complexe. La révolution numérique est garante de sécurité, mais se présente aussi comme chargée de lourdes menaces, comme de nouvelles formes de criminalité, très réactives. Ces menaces affectent l'échelle internationale et demandent une parade à ce niveau. Le cyberdéfense, domaine encore flou, devient importante, sinon décisive. Nous entendons cependant engager la recherche dans le sens de la prospective. Cela s'avère cependant difficile car l'histoire semble nous conduire vers un monde de plus en plus incertain.

En définitive, la révolution numérique ne pose pas seulement de nouveaux défis au droit mais elle modifie la perspective même de son élaboration et de son application dans un contexte complexe, mouvant et imprévisible, où la capacité d'adaptation semble devenir le critère dernier. Qui plus est, il faut cultiver l'ambition mais aussi l'humilité, dans des prises de décision et la mise en place de règlementations nécessaires mais dont le contenu précis ne s'impose pas avec évidence mais relève souvent du moindre mal.

Mots clés :

Cybersécurité, Smart cities, Emirats Arabe Unis, Sécurité et liberté, Numérique, Démocratisation, Big data, GAFAM, Blockchain, Fédéralisme, cybercriminalité, Piratage informatique, bitcoin, Piratage informatique

Summary

The thesis intends to discuss all the implications of the digital revolution in the United Arab Emirates, from a legal perspective. In view of the current situation, particular emphasis is placed on the threat of cybercrime. How can it be prevented as the techniques of aggression continue to improve over the years?

On the one hand, in our thesis, I try to draw a panorama of the existing, namely the history and the particular situation of the Emirates, without forgetting the federal character of its institutional structure. It is also essential, in a more global way, to make an overview, of course always to be completed and changed, of the different aspects, positive and threatening of the digital revolution.

Since the country under study is at the beginning of the implementation of legislation in this field, attention is paid to the way in which other countries, especially France and the United States, are taking up these new challenges. In an attempt to move forward in a comparative manner. It is obvious that the digital revolution is embodied differently depending on the country concerned, and also the moment it is going through. But the local dimension always refers to a global dimension in an increasingly interconnected world. Hyper-globalization, despite moments of retreat, makes legislation on such a vast scale both imperative and delicate.

Upstream, a reflection is carried out on the way in which the law can and must face very complex stakes, requirements in tension, if not dilemmas for example between more security and a fully preserved freedom. In an ever-changing context. Downstream, the digital revolution does not only consist of dangers but allows undeniable progress in the direction of more democratic participation, more efficiency and coordination.

In fact, the balance is nuanced and complex. The digital revolution is a guarantee of security, but it is also fraught with serious threats, such as new forms of crime, which are highly reactive. These threats affect the international scale and require a response at this level. Cyber defence, still a vague field, is becoming important, if not decisive.

However, we intend to engage research in the sense of foresight. However, this is difficult because history seems to lead us towards an increasingly uncertain world.

Ultimately, the digital revolution not only poses new challenges to the law, but also changes the very perspective of its elaboration and application in a complex, shifting and unpredictable context, where adaptability seems to become the ultimate criterion. Moreover, it is necessary to cultivate ambition but also humility, in making decisions and implementing regulations that are necessary but whose precise content is not self-evident but is often the lesser evil.

Keywords: Cybersecurity, Smart cities, United Arab Emirates, Security, and freedom, Digital, Democratization, Big data, GAFAM, Blockchain, Federalism, cybercrime, Hacking, bitcoin, Hacking

Liste des abréviations

AFP	Agence France-Presse
ANSSI	Agence nationale de la sécurité des systèmes d'information
ANSSI	l'agence nationale de la sécurité des systèmes d'information
ATC	Advanced Technology Investment *Company*
ATM	Asynchronous Transfer Mode
BTC	Bitcoin
CNAP	Centre National d'accession à la propriété
CNIL	Commission nationale de l'information et des libertés
CSA	Conseil supérieur de l'audiovisuel
CTIIC	Consolidat infoormation technology infrastracture contract
DCPJ	la direction centrale de la Police judiciaire
DGSI	La direction générale de la Sécurité intérieure
EPC	équipe de protéctioncollective
FED	Fédéral réserve
FMI	Le Fonds Monétaire International
GAFAM	Google, apple, Facebook, Amazon et Microsoft
GAFI	Groupe d'action financière
IA	intelligence artificielle
IP	internet Protocol
KYC	*Know Your Customer*
LLT	Limited Liability Company
LDC	Louis Dreyfus *Company*
NESA	la *National Electronic Security Authority*
NSA	américaine National Security Agency
OIV	Opérateurs d'importance vitale
OSE	Organisation des services d'enseignement
PRT	Personal Rapid Transit
RAT	Remote administration tool
SDAT	la sous-direction anti-terroriste

Sommaire

INTRODUCTION

1 L'histoire semble connaître une certaine accélération, avec le bouleversement inédit des nouvelles technologies. Nos lycéens se demandent aujourd'hui comment leurs aînés ont bien pu vivre sans cette révolution numérique, sans téléphones portables, ni tablettes, ni *high tech*. Paraît ainsi se concrétiser cette prophétie de l'écrivain anglais *Lewis Carroll* : *« pour rester sur place. Il faut courir. Et si vous voulez aller ailleurs, il vous faut courir au moins deux fois plus vite* ». Dans ce contexte, la recherche change également de contours, de contenus, et aussi, bien entendu, de rythme. Les grands enjeux éthiques et politiques, ainsi que les dispositifs juridiques à mettre en place et les pratiques y afférant, ne peuvent être traités abstraitement, indépendamment de cette nouvelle donne. D'une certaine manière, le cadre contextuel les modifie, les déplace et les situe autrement. Et, réciproquement, la révolution numérique représente non seulement un progrès technique à étudier sous cet angle mais aussi le croisement des enjeux variés et importants ne pouvant être occultés dans une réflexion éthique et politique. Les nouveaux défis qui se posent regardent aussi bien le droit public que le droit privé, l'organisation et le fonctionnement des organismes de l'Etat dans le souci de l'intérêt général comme tel que les relations entre les différentes personnes physiques ou morales, notamment dans le contexte du travail. Par ailleurs, un nouvel espace de criminalité s'élargit et se précise de plus en plus, justement celui de la criminalité, rendant indispensable une politique coordonnée à tous les niveaux et des avancées du droit pénal, en fait peut-être provisoires tant des futures évolutions sont à venir encore.

2 C'est donc devenu une quasi-évidence que l'ère du numérique façonne un monde bien différent, qui évolue avec une rapidité inédite. On peut même penser au développement d'une sorte de monde parallèle qui serait le cyberespace à moins que ce dernier ne soit en fait une forme d'intrication d'une multitude de cyberspaces qui toutefois se croisent. Chacun vivrait alors dans son propre cyberespace mais ne serait pas pour autant isolé des autres, au contraire. Les différents cyberspaces seraient du reste mouvant. D'importantes mutations impliquent des évolutions juridiques déjà advenues, ou en cours, ainsi que des modifications à envisager, qui seront sans doute indispensables. On peut même se demander s'il suffit, de prendre en considération l'ampleur de cette révolution, de procéder à des réajustements et à des corrections de trajectoire, ou s'il ne faut pas plutôt envisager d'inventer un nouveau contrat de société, tant les défis qui émergent font éclater les limites de cadres juridiques et de directives, certes fort utiles et salutaires, mais qui donnent parfois l'impression d'être dépassées dès lors qu'elles sont

adoptées. En outre, il n'est pas à exclure. Certes l'hypothèse est radicale et embarrassante pour les juristes- que d'une certaine façon la verticalité même du droit finisse par être mise en cause, sinon pratiquement, du moins concrètement, dans la réalité. Le développement de la cybercriminalité risque de s'accélérer en nous conduisant à une sorte d'impasse, ou en tout cas constitue un défi imposant des évolutions radicales et accélérées. Dans un tel contexte, des mesures juridiques peuvent être inefficaces, voire contre-productives, à l'instar de ce qui s'est passé aux Etats Unis après la décision de prohiber l'alcool en 1919 source , ce qui a poussé des réseaux criminels à se constituer et à trouver des nouvelles façons pour enfreindre la loi.

3 Indépendamment même de la cybercriminalité proprement dite, des points délicats semblent cependant appeler des dispositions législatives comme la protection de la vie privée, la défense d'un éventuel droit à l'oubli rendu fort problématique par la conservation des données, mais également l'efficacité des politiques publiques et des entreprises privées, enjeu devenu plus brûlant dans le contexte de l'hyper-mondialisation et donc d'une concurrence au niveau international. On sait que, depuis une trentaine d'années, la quantité de marchandises échangée à l'échelle planétaire a été multipliée par quatre. Le commerce international représente plus du tiers du PIB mondial. La dématérialisation des échanges et de services dope encore davantage cette évolution. L'épidémie toute récente du Coronavirus nous plonge davantage de perplexité face la mondialisation et entretient en ayant une certaine nostalgie d'un monde plus cloisonné, avec des espaces définis, mais il est néanmoins difficile de penser qu'elle puisse inaugurer une contre- évolution de fond sur le long terme. Bien entendu, l'hyper-mondialisation ne se mesure pas seulement quantitativement mais aussi qualitativement. Elle traduit une évolution importante de la manière même dont s'opère le système de production et d'échange, caractérisée par une perpétuelle surenchère. Cette surenchère implique une exigence d'adaptation sans cesse renouvelée à une donne de plus en plus différente et complexifiée, et aussi, ou même surtout, à une concurrence entre institutions, mais également entre pays. Par ailleurs, on assiste à l'extension d'un nouveau travail à la chaîne, si l'on peut dire, cette fois non seulement au niveau local, mais à l'échelle mondiale. Concrètement, les différentes opérations et étapes d'un processus de production sont divisées et même segmentées en différents points de la planète de sorte que se dessine une nouvelle géographie du monde. On réalise combien cela est vrai des *iPhones Apple* où la logique préside au choix des lieux est évidemment toute pragmatique et centrée sur la rentabilité et l'intérêt financier. Cette hyper-mondialisation ne se réduit certes pas à l'harmonisation des taxes douanières, mais implique

souvent de surmonter des barrières « non-tarifaires » parfois complexes, comme des normes sanitaires ou des régulations de la concurrence. Un régime qui exige donc une meilleure coordination entre les entreprises et les Etats, mais aussi, de façon plus large, entre tous les partenaires de cette institution. Sans oublier des « partenaires » moins engageants comme ceux que connaissent la cybercriminalité.

4 C'est précisément cette interrogation qui nous conduit à une recherche concernant le pays dont nous sommes originaires et citoyens. En effet, c'est bien au niveau de chaque état qu'une législation spécifique, précise et adaptée avec ses nécessités et sa structure, ceci doit relever le défi de l'encadrement, adapté ni étouffant, ni complaisant, d'une dynamique qui n'en est qu'à ses débuts, lorsque même que l'enjeu comporte évidemment – et presque toujours une dimension internationale intégrable autant qu'inéluctable. L'entreprise s'avère passionnante, car elle nous entraîne dans le processus d'un tourbillon en cours autant qu'elle nous oblige à l'anticipation, et nous interdit la passivité. A défaut d'une vraie régulation juridique, au moins *a minima,* la révolution numérique pourrait entraîner des conséquences encore difficiles à mesurer aujourd'hui. En même temps, l'avancée de l'histoire nous donne une sorte de tournis et le sentiment de ne plus pouvoir maîtriser une évolution, d'un côté hautement souhaitable, mais de l'autre inquiétante et qui peut même donner le vertige. Il semble parfois que l'avancée des progrès numériques condamne à être décalée et donc inefficace toute réglementation, forcément en retard par rapport au problème qu'elle entend résoudre, et donc vite inadaptée. C'est pourquoi le devoir qui nous incombe est celui d'un discernement, d'une évaluation, entre diabolisation et exaltation, au-delà de réactions passionnelles d'enthousiasme ou de peur, sinon de panique, qui doit tenir compte de la diversité des cas et des situations, mais dégager aussi quelques principes d'orientation, afin de poser des jugements circonstanciés. Une ambition qui n'est pas mince. Certaines questions éthiques sont faciles à identifier. Pour autant, la réponse ne semble pas évidente. Par exemple, comment vont s'équilibrer dans une société du numérique l'intérêt général et l'intérêt particulier ? Comment faire face à une possible dictature de la transparence à supposer que cela soit encore possible sinon peut-être par dissimulation ou falsification ? Si l'on peut aisément définir en droit la sphère privée comme étant celle dont chacun est libre de refuser l'accès à autrui, ne peut-on simplement redouter que la possibilité concrète d'un tel refus soit aujourd'hui en péril ? Le télescopage entre l'idéal de confidentialité et celui de service public peut-il être régulé ? Un pouvoir politique mal intentionné et soucieux du contrôle des citoyens ne risque-t-il pas de se servir des nouveaux atouts du numérique pour

mieux encadrer encore de façon autoritaire, sinon totalitaire, son pays? Sans sombrer dans une sorte de paranoïa qui conduit à se sentir constamment observé et sous surveillance, ne faut-il pas mesurer aujourd'hui le risque d'un véritable "Big Brother" contrôlant tout comme dans le roman d'anticipation "1984" de George Orwell? Des voies de solution peuvent sans doute se dégager autour de la notion de « domanialité », à savoir ce qui concerne en propre le domaine de l'Etat, au moins quant aux principes. Cette notion permettrait de tracer une limite entre ce qui relève de l'Etat et tout le reste, qui ne devrait donc pas être contrôlé d'une telle façon. Ainsi, ce qui relève de la domanialité devrait être préservé des intérêts privés. En revanche, ce qui n'en relève pas, ne devrait pas être soumis à un contrôle et encore moins à une domination des pouvoirs publics. Pour autant, ce principe posé, les différents problèmes particuliers semblent toujours se poser de façon difficilement décidable car la protection et la vocation spécifique de ce qui est propre à l'Etat n'implique pas toujours clairement le « comment » dans le détail, surtout en regard de la diversité des différents systèmes politiques et des histoires qui les façonnent en profondeur. Il semble ainsi que la révolution numérique rende en fait plus aigus et plus délicats différents problèmes où s'articulent la dimension éthique et le juridique proprement dit, en les complexifiant encore. A l'évidence, l'encadrement juridique des données ne saurait se limiter à envisager l'aspect purement pratique, l'efficacité ponctuelle, mais pose la question des valeurs à respecter, ou même à promouvoir. Dans le cadre du droit privé, quel statut juridique reconnaître aux données personnelles, de soi extrapatrimoniales pour le moment, échappant donc au champ de l'échange et du commerce, mais que l'on pourrait éventuellement considérer comme relevant de la propriété éventuellement commercialisable de l'individu ? Toujours en ce qui concerne les données, leur conservation sous la forme du *cloud computing* inaugure une sorte de période nouvelle dans l'ère elle-même nouvelle du numérique, avec des questions spécifiques. Or, donc, des aspects particuliers demandent ainsi à être étudiés et traités comme celui du droit d'auteur dans un univers numérisé, ou encore celle du statut des métadonnées. Ces dernières, on le sait, sont des informations périphériques aux données, visant à les décrire dans leur contexte, et ainsi à les situer, et à les rendre plus intelligibles, comme l'étiquette d'un vêtement qui en présente la texture ou la taille. De fait, beaucoup de fichiers, de documents et de données, sont aujourd'hui oubliés en raison de leur mauvaise contextualisation. Mais le développement des métadonnées ne conduit-il pas à tout enserrer dans un filet empêchant jamais le droit à l'oubli ? Ainsi, ce que l'on appelle quelquefois le cyberespace ne conduit-il pas à favoriser de nouvelles formes de conflictualité, y compris le terrorisme ?

5 Notre recherche vise donc principalement à évaluer l'impact de la révolution numérique sur les politiques publiques des Émirats arabes unis, d'une part dans la perspective d'une plus grande efficacité, mais aussi, d'autre part, dans la volonté concrète d'une véritable big data

de la gouvernance des Etats. Elle s'élargit aux questions relevant plutôt du droit privé. Du reste, la transparence des données n'est-elle pas susceptible de faire peser de larges menaces sur les relations entre un employeur et ses employés par exemple ? Par exemple, une connaissance facilitée des problèmes de santé d'une personne pourrait contribuer à sa discrimination à l'embauche. Ainsi, notre recherche suppose-t-elle un inventaire de la situation présente, dans l'idée d'une évaluation qualitative, éthique, politique et juridique. Mais elle s'oriente aussi dans la direction de préconisations à envisager. Bien entendu, elle doit au préalable prendre en compte les spécificités des Émirats, historiques, culturelles et politiques, les rythmes qui lui sont propres, l'état d'avancement de la révolution numérique qui est le sien. L'impact du numérique ne saurait évidemment être le même selon les pays, même s'il faut garder également à l'esprit que les pays qui peuvent être encore en retard, ne le seront pas toujours et indéfiniment, mais au contraire vont rattraper bien vite ce retard. Les résultats, tout comme les espoirs suscités, tiennent à de nombreux facteurs, qui plus est évolutifs. Un fort coefficient d'imprévisibilité affecte tout diagnostic sur le futur. Cela ne nous dissuade cependant pas de dégager des hypothèses, et de signaler des enjeux et des défis, peut-être des inquiétudes, mais également des solutions possibles.

6 Le bouleversement numérique est polymorphe, mais également paradoxal. Il ne se limite évidemment pas à l'essor des techniques numériques, mais conduit à la fois à refaire de la planète entière un village en réseaux[1] tout en contribuant en même temps à une véritable décentralisation dans l'échange, les différents niveaux communicants par ailleurs entre eux. Ainsi, l'articulation en réseau du fonctionnement d'une grande ville se connecte au grand logiciel du monde entier. Cela est déjà singulièrement le cas de villes comme New York, Mexico City, Londres ou Paris.

7 On peut définir la révolution numérique par une mise en relation, au niveau planétaire, des individus grâce aux nouveaux moyens de communication, au travers d'une circulation de

[1] Comme l'avait déjà montré Marshall McLUHAN, *Guerre et Paix dans le village planétaire*, tr. fr. Paris, Robert Laffont, 1970.

l'information et d'un processus de numérisation. Ce dernier dépasse largement le mode analogique, en rapidité et en efficacité, de sorte que l'on parle quelquefois des autoroutes de l'information. D'un point de vue pratique, et ce immédiatement, les atouts pratiques sont bien entendu de première importance. Il faut de toute manière prendre acte de l'ampleur considérable de l'évolution, qui se présente en définitive comme une véritable révolution culturelle, comme un tournant civilisationnel, comparable, sinon supérieur en son étendue, à la découverte de l'imprimerie (oui du moins de l'usage de lettres mobiles pour imprimer) par Gutenberg au milieu du quinzième siècle à toutes les échelles de la vie sociale, sans oublier la plus intime désormais moins protégée, y compris d'ailleurs au niveau de l'organisation des savoirs et de l'utilisation des facultés cognitives[2]. En outre, toute information peut être numérisée de sorte que nous sommes bien en présence d'une mutation globale, touchant, ou du moins pouvant toucher, tous les secteurs. Autrement dit, toutes les informations peuvent être exprimées et circuler au travers d'une combinaison de nombres [3]et ce grâce à des appareils très divers, et de plus en plus diffus dans la population. On peut dire que cette révolution a commencé progressivement dans les années 1980s, effrayant souvent les générations plus âgées, désemparées parfois par de nouvelles façons de communiquer mais également de régler des affaires pratiques, ne serait-ce qu'acheter un billet de train, avant d'exploser, en particulier dans la deuxième moitié des années 90s, grâce à internet, le « réseau des réseaux », sans négliger l'effet plus récent encore des smartphones. Au départ projet politique, celui d'ARPANET, internet est devenu notre nouveau monde aujourd'hui. Cette révolution s'étend à toute la planète même si c'est de façon inégale selon les pays, avec des rythmes différents, mais également avec un phénomène de rattrapage, les pays les plus en retard s'efforçant de réduire leur infériorité technique en la matière. Les échanges sont donc facilités à tous les niveaux et à toutes les échelles. Toutefois, les avantages pratiques, qui sont évidents, ne vont pas sans susciter des remarques critiques, de la part de ceux que l'on peut éventuellement considérer comme technophobes mais qui se situent souvent à un autre niveau d'appréciation et d'évaluation, d'ordre éthique cette fois, de même que les sociologues distinguent souvent deux types de rationalité, motivant les choix faits, d'une part par la rationalité instrumentale, en vue de l'intérêt, et d'autre part la rationalité axiologique, soucieuse du respect des valeurs[4]. Il faut donc s'interroger de façon à la fois systématique et circonstanciée sur la façon dont est aussi reçue,

[2] Cf. Michel SERRES, *Petite Poucette*, Paris, Le Pommier, 2012.
[3] En l'occurrence 0 et 1.
[4] Raymond BOUDON, *Essai sur la théorie générale de la rationalité*, Paris, Presses Universitaires de France, 2016.

vécue et inculturée, à savoir adaptée au cadre culturel local toujours singulier, la « révolution numérique », en fonction du contexte et sans doute des politiques menées.

8 Il va de soi que l'administration d'un pays, tout comme d'ailleurs le management d'une entreprise, peuvent être considérablement transformés par le numérique, au point d'ailleurs de marginaliser certains acteurs, individuels ou collectifs, qui rencontrent des difficultés à intégrer certaines mutations. Des problèmes épineux peuvent apparaître, ne serait-ce que celui de la signature électronique et des litiges qui l'entourent. Les téléservices constituent certainement l'aspect immergé de l'iceberg, le plus visible par tous. Mais l'évolution la plus fondamentale est au niveau des centres de données étatiques. La complexité du monde des échanges, et surtout son développement, entraîne ainsi une complexification des processus administratifs, donc des administrations elles-mêmes qui les gèrent, rendant souhaitables une simplification et un ajustement. En France, il est d'usage de regretter l'engorgement fréquent et récurrent des services administratifs, comparés volontiers à une improbable « usine à gaz ». A l'évidence, l'administration peut être considérablement simplifiée et rendue plus cohérente, dans tous les pays, grâce au numérique, même si dans un premier temps, les efforts d'adaptation peuvent en effet sembler difficiles à certains, anxiogènes, sinon des pertes de temps et d'énergie. Mais c'est dans un premier temps seulement, comme ce fut le cas, on le sait, lorsque la SNCF, en France, a mis en place entre 1993 et 2003 un nouveau système de réservation, [5] remplaçant l'ancien système devenu obsolète, RESA, pour ouvrir à un autre système RESARAIL dix ans plus tard. Souvent présenté comme un échec, SOCRATE traduit en fait un moment de tâtonnement avant une modernisation dont les effets bénéfiques sont visibles à long terme.

9 La rapidité et l'importance de la révolution numérique ne sont donc plus à établir. Les mutations profondes se sont déroulées en amont des petites manifestations au quotidien, constatables par tous, parfois déroutantes, notamment, nous l'avons dit, pour les plus âgés, mais aussi pour les personnes les moins diplômées et les moins formées – avec un risque de nouveau clivage social - , parfois, en revanche, grisantes voire aliénantes, surtout pour les nouvelles générations, formant un contexte véritablement nouveau. On peut se demander si le numérique ne favorise pas des conduites compulsives et addictives. Ainsi, lorsque l'euphorie pousse à rendre publique une donnée personnelle gênante, par exemple sur Facebook ou sur un site, par la suite difficile

[5] Un acronyme de Système offrant à la clientèle des réservations d'affaires et de tourisme en Europe.

à effacer, ou au travers des divers jeux vidéo. L'immédiateté favorisée peut aussi entraîner des dérapages verbaux, faute d'un temps de réflexion et de recul qui les aurait évités. Désormais, en tout cas, les données ne peuvent plus être aussi facilement que jadis retenues prisonnières de quelques-uns. Qu'on le veuille ou non, l'ouverture de plus en plus large des données aux publics, y compris de façon illégale comme dans le cas du « Wikileaks », contribue à faire émerger une véritable démocratie numérique, ou du moins à en faire retentir l'exigence. La tentation pourrait être alors de crier « victoire » trop tôt et de considérer de façon unilatérale l'essor du numérique comme un processus uniquement positif, comme un progrès incontestable à tous égards. Les études menées actuellement sur les implications de l'ère du numérique sont autrement nuancées : par exemple celles conduites dans le cadre des éditions IMODEV sous la direction d'Irène Bouhadana et de William Gilles. En effet, si, à l'évidence, de nouvelles possibilités apparaissent, de nouvelles questions se posent également, et de nouveaux risques sont discernés. « Laisser penser que la révolution numérique créerait un renouveau de la démocratie grâce aux recours aux nouvelles technologies est illusoire »[6]. Une littérature assez saisissante, depuis Aldous Huxley dans Le *meilleur des mondes* sonne l'alarme quant aux risques de déshumanisation, de création d'un monde robotisé et inhumain. L'homme semble en danger d'être réduit à l'état de rouage d'un système complexe, bref de devenir un objet. Plus largement, l'infrastructure technique et son développement, à une vitesse sidérale et sidérante, renouvelle non seulement les façons de vivre mais de penser. Ils suscitent une tout autre conception de l'homme et de son futur qui s'exprime en particulier, sous sa forme la plus méliorative, dans ce que l'on appelle le « transhumanisme », célébrant une sorte de pouvoir démiurgique de l'homme. Cet arrière-fond philosophique, qui demanderait un traitement spécifique, global et approfondi, et concerne peut-être, de façon encore plus urgente et déchirante, la techno médecine, ne peut ici être thématisé de façon systématique et détaillée [7] mais demeure le cadre dans lequel beaucoup de réflexions et d'enjeux, que pour le coup nous étudierons, ne manquent pas de s'inscrire. Certaines décisions juridiques demandent au préalable une réflexion d'ordre proprement philosophique et éthique, bien au-delà des cadres déjà tracés.

[6] William GILLES, « Démocratie et données publiques à l'ère des gouvernements ouverts : pour un nouveau contrat de société ? », in *Droit et gouvernance des données publiques et privées à l'ère du numérique*, les éditions IMODEV, Paris, 2015, 16 [15-32].

[7] Ce que fait en revanche le philosophe Luc Ferry : Luc FERRY, *La révolution transhumaniste. Comment la technomédecine et l'ubérisation du monde vont bouleverser nos vies*, Paris, Plon, 2015. En plus incisif et engagé encore : Laurent ALEXANDRE (avec Jean-Michel BESNIER*), Les robots font-ils l'amour ? Le transhumanisme en 12 questions,* Paris, éd. Dunot, 2016.

10 Il semble à tous égards que le tournant numérique puisse être vraiment considéré comme irréversible, sauf improbable catastrophe mondiale, sorte de bug informatique planétaire. Fondamentalement, il convient de rappeler au préalable, quoiqu'on puisse penser d'elles et des potentialités qu'elles multiplient, que les nouvelles technologies restent malgré tout de l'ordre de l'instrument et de l'outil. On peut songer à la fameuse langue d'Esope. Celui-ci, à la demande de son maître, qui lui enjoignait de lui préparer la pire des choses, prépara…de la langue. Et à la demande de son maître de lui préparer, cette fois, la meilleure des choses, il confectionna à nouveau de la langue ! Cela veut dire tout simplement qu'un instrument, une possibilité, ne sont ni bons ni mauvais en eux-mêmes, mais le deviennent, et vont du meilleur au pire, en fonction de l'usage qui en est fait. Cette ambivalence probable de la révolution numérique défie toute doxa, c'est-à-dire toute tentative de donner une opinion tranchée, trop simple. Elle nous force non seulement à une réflexion subtile et à des distinguos mais encore à un inventaire très détaillé de l'existant. Elle ajoute ainsi une difficulté supplémentaire à notre recherche, mais lui donne aussi, nous semble-t-il, toute sa pertinence. C'est en effet la tâche propre du droit public et du droit privé d'établir le cadastre formel dans lequel s'inscrit une bonne pratique du numérique.

11 Sans aucun doute, cette prise en compte de l'ambivalence intrinsèque d'un instrument, surtout si sophistiqué et performant, oblige-t-elle à poser la question des risques. Or, les risques éventuels peuvent tenir d'une part à de mauvaises intentions, mais également, d'autre part, à de bonnes intentions - dont on sait que l'enfer en est pavé – mais mal conduites, avec une mauvaise maîtrise des instruments, comme celui qui se blesserait en maniant une hache pour couper du bois. La tentation peut être grande alors de se référer au « principe de précaution » dont parle le philosophe Hans Jonas[8]. En suivant cette logique, il faudrait prêter plus d'attention aux risques qu'aux chances, car le risque peut être fatal tandis que la simple omission d'une chance ne constitue jamais qu'un manque, et donc se prémunir surtout contre les nouvelles technologies, plutôt que saisir les opportunités nouvelles avec audace ou témérité. Il convient de noter qu'il s'agit là d'une réflexion éthique de fond qui concerne bien des secteurs et non pas un seul, unique. Ainsi le débat est-il vif sur les OGM ou le nucléaire. Dans le cas des données collectées, le problème est bien entendu quelque peu différent. En effet, dans le nucléaire par exemple, l'étendue de conséquences éventuelles semble considérable et

[8] Hans JONAS, *Le principe responsabilité*, Paris, tr.fr, Champs Flammarion1990. Pour une évaluation critique : Luc FERRY*, Le nouvel ordre écologique*, Paris, Grasset, 1992.

totalement impossible à maîtriser, imprévisible, dépendant par exemple du vent en cas de catastrophe orientant la diffusion des éléments nocifs. Mais il est vrai également que l'instrumentalisation perverse de données faciles à connaître pourrait entraîner des conséquences en cascade elles-mêmes imprévisibles, et surtout contribuer à une dérive dictatoriale et totalitaire. Dans le cadre du droit privé, une personne mal intentionnée pourrait par exemple nuire à une autre en diffusant des données nuisant à sa réputation ou une entreprise pourrait très aisément discréditer une concurrente. Qui sait en effet quel usage pourraient faire aussi bien des services publics que des organismes privés de données parfois fort confidentielles, surtout compromettantes ? Par exemple les opinions intimes des citoyens ou leurs mœurs. C'est ainsi qu'envisager les bienfaits de l'ère du numérique oblige à songer aux nécessaires garde-fous à poser, sinon à des antidotes juridiques. En tout cas, un état de droit doit garantir qu'aucune exploitation illégale ne sera faite de données collectées. A plus vaste échelle, celle des Etats par exemple, les risques de piratage et de criminalité peuvent induire des conséquences considérables voire à l'arrivée bouleverser l'ordre du monde et c'est pourquoi cet aspect doit être spécialement développé dans notre thèse.

12 Mais la question qui est susceptible de contenir des menaces et des dérives possibles ne saurait occulter le fait que beaucoup de citoyens se réjouissent aussi des opportunités pour eux d'être mieux informés et de contrôler ceux qui les gouvernent. Le droit doit-il uniquement fixer des limites ou aussi valoriser des opportunités ? Comment l'avenir ou déjà la jeunesse d'un pays considéreraient-elle une génération surtout préoccupée de se protéger de risques éventuels au prix du sacrifice de futurs plus ouverts voire enchantés ? Les dangers réels et potentiels, le revers de la médaille, ne peuvent en faire négliger le bon côté. On peut ainsi dire que l'essor du numérique libère de fait la parole publique et contribue ainsi à créer un contexte de liberté et de développement personnel. Il n'est plus aussi facilement possible de maintenir des peuples dans l'ignorance, ou dans le silence que jadis, ce qui relance le désir d'une nouvelle efflorescence, dans le sens d'une vraie participation de tous, ou au moins d'un plus grand nombre. Néanmoins, le développement d'internet accule aussi l'homme à une nouvelle aventure au travers de terres inconnues, face à de nouveaux défis, et à une prolifération qui n'en est peut-être qu'à ses débuts de ruptures idéologiques, de mouvements de contestation très négatifs qui peuvent aussi fragmenter nos sociétés et nos états de sorte qu'il faut en quelque sorte trouver une boussole pour entreprendre une odyssée sur la toile pas moins périlleuse que celle d'Ulysse après la

guerre de Troie[9]. La revendication peut même fleurir d'une nouvelle démocratisation de la vie d'un pays, ou d'une ville, presque d'un retour à la démocratie directe, après le détour vers des formes de démocratie représentative ne tenant les populations informées qu'avec parcimonie. En ce sens, qui sait, l'avenir pourrait être à un recours plus fréquent au référendum, consultation de tous les citoyens sur une question, comme celle, lourde de conséquences, du Brexit en juillet 2016. Une telle évolution pourrait modifier de façon durable le fonctionnement institutionnel des Etats. Cette évolution peut être perçue positivement comme étendant l'exercice de la démocratie ou, au contraire, négativement, comme favorisant l'instabilité en raison de la versatilité des opinions publiques, surtout en temps de crise. Du reste, la démocratie représentative, au sein de laquelle le pouvoir souverain du peuple présente l'avantage régulateur d'être différée puisque exercée par des représentants élus, avec les délais de réflexion et de recul souhaitables. Toutefois, même dans une monarchie par exemple, la consultation de l'opinion peut aussi être utile et bénéfique pour le pouvoir exécutif. Dans le cas spécifique des Emirats qui est celui d'un état fédéral dont le bon fonctionnement dépend en bonne part de la synergie entre l'échelon fédéral et l'échelon local, la consultation revêt une importance peut-être encore plus décisive, et ce en considération également de la volonté affichée d'une gouvernance participative qui soit l'expression ajustée de la volonté des citoyens. Dans la mesure où les Emirats ne sont pas une simple confédération, mais un véritable état fédéral, des décisions importantes sont prises à ce dernier niveau, pour des raisons d'efficacité, mais en lien constant avec les opinions populaires à l'échelle de chaque entité régionale, comme par un mouvement de systole et de diastole. Depuis les récentes élections de 2006, la moitié de la chambre des Emirats est désignée de façon totalement démocratique, ce qui traduit une évolution du régime et du pays que peut relayer le développement numérique. Opérant une fusion originale et en devenir entre tradition et modernité, oscillant entre ces deux pôles pour asseoir un équilibre jamais complètement acquis, les Emirats tracent une voie qui leur est propre, à tous égards, et dont les atouts du numérique permettent une reconfiguration constante pour l'améliorer et l'ouvrir davantage encore.

13 De toute manière, l'avènement du numérique transforme les rapports entre gouvernants et gouvernés, à l'avantage ou au détriment des uns ou des autres, et, on l'espère, à l'avantage des deux dans un scénario « gagnant-gagnant », ce qui constitue le résultat à rechercher, et la

[9] Cf. Guillaume CAZEAUX, *Odyssée 2.0. La démocratisation dans la civilisation numérique*, Paris, Armand Collin, 2014.

condition d'une viabilité dans la durée, car le mécontentement d'une partie provoque à plus ou moins long terme, de façon inévitable, des dysfonctionnements voire des troubles graves et des crises dangereuse. D'une certaine façon, il semble même possible de parler de « transition démocratique », certes non pas au sens du passage d'un régime non-démocratique à un régime démocratique, mais de l'évolution entre deux formes de démocratie, dont la seconde serait plus assurée, durable et sincère. On pourrait la qualifier de "participative", cette participation étant rendue possible par les nouvelles technologies. On sait que Rousseau, au siècle des Lumières, raille les Anglais qui se croient libres, et artisans des décisions prises, alors qu'en vérité ils ne le sont qu'au jour où ils élisent leurs représentants[10]. Dorénavant, grâce au numérique, les peuples pourraient enfin prendre réellement part aux décisions prises. Il est toutefois légitime de se demander à cet égard si la mise en place d'un système de démocratie directe peut s'appliquer à l'échelle d'un grand pays ou ne convient pas seulement à de plus petites échelles comme celle d'une école, d'une entreprise, d'une association, d'une ville à taille humaine éventuellement. Ce n'est pas pour rien si en 1787 la constitution américaine tourne le dos à l'utopie de la démocratie directe et lui préfère d'emblée un système dont le pivot est la représentation élective. De plus, la démocratie représentative permet de prendre distance et recul, de s'inscrire dans une certaine durée et d'éviter aussi l'emballement immédiat. En tout cas, le bouleversement introduit par le numérique ne constitue-t-il pas un horizon entièrement nouveau ? Du reste, cette nouvelle sensibilité des citoyens fait écho aux perspectives tracées par des philosophes de l'école de Francfort, en Allemagne, celles d'une éthique communicationnelle comme Apel ou Habermas[11].

14 Toujours est-il que les gouvernés semblent poussés par le développement des nouvelles technologies à exiger des gouvernants le respect d'une plus grande déontologie contrôlable par les nouvelles technologies. D'une certaine façon, les instances au pouvoir doivent davantage rendre compte de ce qu'elles font et de leur fortune, d'autant plus que la crise financière et la précarisation des classes moyennes rendent davantage insoutenables des formes cachées d'enrichissement. D'ailleurs, il s'avère davantage possible de les surveiller. On pourrait évoquer là une exigence de transparence, qui n'est pas entièrement nouvelle, mais qui se fait de plus en plus forte en raison également de nouvelles possibilités de contrôle. Il y a comme une sorte de

[10] *Contrat social*, III, 15.
[11] Karl-Otto APPEL, *Ethique de la discussion*, Cerf, Paris, 1994 ; Jürgen HABERMAS, *Théorie de l'Agir communicationnel,* Fayard, tr.fr. 1987.

dialectique complémentaire entre une évolution des mentalités et l'explosion des possibilités technologiques. L'une appelant en quelque sorte l'autre. Les volontés de contrôle concernent en particulier, en Europe occidentale, dans le contexte de graves difficultés économiques, les questions des revenus et des patrimoines des gouvernants, rendues brûlantes par la pression fiscale. L'idée sous-jacente, au-delà d'une éventuelle curiosité teintée d'envie, semble bien être celle de l'affermissement de la démocratie, qui implique l'intégrité ! Dans les Emirats, le problème se pose un peu différemment en raison d'une histoire récente - car le pays n'existe comme tel que depuis une quarantaine d'années - mais aussi du bon niveau économique et financier dans l'ensemble, ce qui évite trop de frustrations, donc de crises sociales et de revendications nouvelles. L'observateur étranger ne saurait négliger le fait qu'un pays qui s'est formé depuis peu de temps dépense plus d'énergie à se configurer, surtout dans un contexte qui est au départ très loin du monde occidental, marqué jadis par d'autres modèles sociaux et des valeurs différentes. Deux univers se croisent : le monde occidental et son idéal démocratique, d'une part, les traditions arabes, de l'autre. Non pour s'affronter, mais pour s'ajuster et se compléter sans se confondre mais en permettant une synthèse harmonieuse dont témoigne au demeurant la loi fondamentale du pays.

15 L'axe problématique de notre recherche se dégage plus clairement en fonction de ce qui précède. D'une certaine façon, le droit public comme le droit privé ne trouvent-ils pas leur légitimité, et même leur nécessité, dans la fonction régulatrice qui leur appartient en propre, en tant qu'ils permettent un équilibre entre des exigences apparemment opposées, ou en tout cas en tension ? Ainsi, il semble indispensable de trouver une voie moyenne entre le seul souci de la transparence de données offertes à tous, et le droit de chacun de préserver sa sphère privée. Cette recherche d'une voie moyenne et d'un point d'équilibre constitue sans doute un des soucis premiers de l'ensemble de notre recherche et d'une interrogation de juriste qui doit sans cesse s'élargir et se renouveler. De même, y-a-t-il une tension entre l'idéal de l'information, et celui de l'indépendance de chacun. D'un point de vue systématique, il semble alors que la tâche spécifique, incontournable et précieuse du droit, soit précisément de garantir cet équilibre minimum, au moins sous la forme d'un moindre mal. La solution trouvée ne sera pas forcément parfaite et encore moins définitive, mais elle permettrait du moins à un moment donné de trouver une solution la moins insatisfaisante possible et susceptible de sauvegarder, toujours dans la mesure, du possible, un certain équilibre face à des menaces réelles ou envisageables.

16 Dans cette perspective de fond, et en tenant compte de la singularité notable des Emirats, il nous semble indispensable d'accorder toute notre attention à trois notions de première importance, évidemment à articuler les unes avec les autres. Ces trois notions gravitent toutes autour de l'idéal, par ailleurs problématique nous l'avons dit plus haut, d'une plus grande accessibilité des données. Les *data* sont des informations dont on a pris connaissance, ou dont on est susceptible de prendre plus ou moins facilement, ou surtout jadis très difficilement, connaissance. La première de ces notions est celle des *open data* ; la seconde des *smart cities*, et la troisième des « réseaux intelligents ». Bien entendu, ces notions ne seront pas étudiées uniquement pour elles-mêmes, mais dans la mesure, et seulement dans la mesure, où elles concernent la situation des EAU.

17 La première notion, celle de l'*open data* désigne comme tel le fait que de très nombreuses données soient disponibles grâce aux nouvelles technologies. On peut dire qu'il s'agit déjà d'un état présent, déjà en expansion croissante, mais également d'une dynamique dont il convient de mesurer l'ampleur et la postérité. En latin, *open data* veut dire "donnée ouverte". Cette donnée peut provenir aussi bien du secteur public que privé. Elle est diffusée de façon ouverte permettant à la fois l'accès de tous et la réutilisation par tous. Les collectivités sont souvent tenues de publier ou de laisser publier certaines données sous forme numérique. Au-delà du factuel, et des opportunités concrètes, l'open data s'inscrit dans une philosophie éthique et juridique bien précise, celle d'un droit véritable à connaître certaines informations. Mais, plus largement, cette philosophie est également celle d'une diffusion élargie de l'ensemble des informations devant en quelque sorte caractériser une nouvelle civilisation, et stimuler de nouveaux échanges, de tous les genres. Se créerait ainsi un monde aux possibles élargis. L'open data concerne enfin tout type de données numériques. A l'idée d'un accès et d'une réutilisation autorisés s'ajouterait celle d'une gratuité, ou au minimum d'un *low cost*. Il est important de souligner que les données en question peuvent aussi bien concerner les politiques gouvernementales que la recherche scientifique. Le phénomène de l'*open data* semble ainsi rompre avec la conviction implicite ou explicite d'un savoir réservé à une élite, auquel le profane, par exemple celui qui n'est ni chercheur ni étudiant, ne saurait avoir accès. L'impact effectif de l'*open data* est d'ores et déjà considérable comme l'atteste l'émergence du projet pour le séquençage du génome humain, suite notamment à un *Open data Consortium*. Depuis la loi étasunienne de 1966 "Freedom of Information Act", la dynamique de l'*open data* ne cesse de se diffuser dans le monde. En Europe, en 2003, une importante directive du Parlement européen

et du Conseil, la directive 2003/98/CE s'inscrit dans un même sens. En 2010, la Sunlight Fondation, organisation américaine sans but lucratif, définit dix critères visant à vérifier qu'il s'agisse bien d'un *open data*. Dans une perspective économique, l'open data doit permettre de favoriser une véritable concurrence.

En ce qui concerne la deuxième notion, celle des « *smart cities* », il y a lieu d'y voir l'utilisation déjà en œuvre et encore à perfectionner des nouvelles technologies avant d'assurer une harmonisation d'ensemble et une coordination plus articulée des instances et des initiatives à tous les plans. On peut qualifier une ville d'intelligente dès lors que les différents éléments de son fonctionnement, par exemple l'énergie ou les ressources humaines, marchent de concert, que les décisions sont prises de façon le plus consensuelle possible et bien entendu la mieux coordonnée, et appliquées de façon participative, tandis que la qualité de vie des citoyens, mais aussi le respect de l'environnement, sont davantage pris en compte. On peut encore estimer que la bonne entente entre le secteur public et le secteur privé, mais également l'articulation harmonieuse entre les différents organismes et entreprises, mais aussi entre individus, constitue aussi une caractéristique importante des *smart cities*, dans la mesure où la synergie ainsi favorisée maximalise l'efficacité des différents projets. La conception de l'Etat qui est celle des Emirats semble correspondre précisément à cette idée d'harmonisation, car elle met en valeur son rôle de catalyseur des initiatives, à tous les échelons. En somme, les *smart cities* sont toujours multidimensionnelles, et ce grâce aux apports du numérique.

18 Le « réseau intelligent » est un système de communication ou de gestion de l'énergie, dont la portée est maximalisée par de nouveaux développements, et qui bénéficie donc d'une portée élargie, ainsi que d'une rapidité multipliée de l'échange. Les réseaux qui se développent permettent une meilleure distribution du produit, plus d'économie, de cohérence, et moins de pertes et de gaspillage. Il est à noter que ces différents réseaux s'interconnectent également entre eux. D'une certaine façon, ils permettent une « réalité augmentée », à savoir une densification du réseau global, qui peut présenter aussi un aspect inquiétant, sinon monstrueux. Bien entendu, ces notions trop complexes et souvent polymorphes ne sauraient être étudiées abstraitement en amont, mais doivent l'être en aval, au travers des réalisations concrètes, chaque fois différentes, même si d'une certaine manière elles suivent un paradigme voisin façonné par le numérique.

19 Ces trois notions peuvent converger en une seule qui présente sans doute la caractéristique d'être plus large et englobante, mais peut-être surtout utopique, sinon asymptotique [12]relevant d'un idéal au service duquel des réalisations concrètes se mettent déjà en place. Il s'agit en l'occurrence de la notion d'un « Etat intelligent » maximalisant les échanges, les informations et la compréhension. C'est autour de lui que peuvent graviter nos réflexions. Il s'agit d'un projet d'ensemble. Une politique doit en effet être mise au service d'un tel « état intelligent », et donc vérifier sa pertinence dans le cadre d'un projet, d'une vision. Il nous semble d'ailleurs que l'adjectif même « intelligent » inclut à la fois l'idée des meilleures connaissances et compréhensions possibles et celle d'une habileté pratique, à savoir l'art d'ajuster les moyens et ressources disponibles et les buts. Bien entendu, en soi, l'Etat n'est pas une personne qui serait sage comme telle mais on peut raisonnablement estimer que l'ensemble des citoyens peut le devenir un peu davantage, dans tous les sens du terme, grâce à la révolution numérique, ou peut-être en partie contre son gré. Il semble cependant opportun de préciser d'ensemble que ce qualificatif d' « intelligent » ne vise pas d'abord ce qui relève de l'ingénierie et des prouesses techniques mais inclut d'emblée et toujours une dimension stratégique et le politique, le désir de faire quelque chose qui ait du sens et réponde à la certaines valeurs.

20 Le numérique est quelquefois présenté comme un « monstre doux ». L'expression remonte à Alexis de Tocqueville dans son célèbre ouvrage sur « la démocratie en Amérique » mais a été plusieurs fois reprise, en particulier récemment par Raphaël Simone[13]. L'expression est oxymorique et fait songer à celle de « soft power ». Le « monstre doux » semble embrasser tous les aspects de notre existence et il prospère grâce aux données qu'il engloutit et conserve. Il semble donner naissance à - ou du moins entretenir - un étrange narcissisme, une complaisance à étaler jusqu'à l'intime, dont Facebook offre l'illustration la plus suggestive. La volonté d'être connecté en permanence ou peu s'en faut conduit à une sorte d'état d'esprit, voire de dépendance, qui forme comme un nuage entourant toutes réalités. Peut-on alors redouter une nouvelle forme de despotisme ? Voire un plan machiavélique de contrôle mondial même si la théorie du complot nous paraît toujours bien aléatoire et bien suspecte ? Faut-il se soumettre à ce monde ou le dompter, si du moins cela est seulement possible ? Autant d'interrogations à faire retentir tout au long de notre étude mêmes si elles ne sauraient être posées en dehors du contexte précis des EAU, en sachant que l'histoire s'accélère et que ce qui se vérifie dans telle

[12] Ce qui relève d'un horizon toujours visé et jamais atteint.
[13] Raphaël SIMONE, *Le Monstre doux : l'occident vire-t-il à droite* ? Gallimard, Paris, 2010.

région de la planète se vérifiera peut-être très rapidement ailleurs. Le numérique semble plus qu'incontournable, mais pour quelle configuration, et pour quelle place laissée à l'homme, ou élargie à son profit, qui sait ?

21 Le développement rapide d'internet permet aussi aux criminels d'explorer de nouvelles pistes d'action et de tisser de nouveaux réseaux. La cybercriminalité, qui à certains égards prolonge en bonne part les formes plus classiques de la criminalité se caractérise d'abord, et simplement, par le moyen utilisé. Le célèbre aventurier vénitien Casanova, au XVIIIe siècle, extorquait de l'argent à une aristocrate parisienne, Madame d'Urfé, en la trompant. Aujourd'hui, avec moins d'élégance peut-être, mais autant d'efficacité, les nouveaux délinquants se servent d'un ordinateur, naviguent dans le cyberespace. La cybercriminalité renferme en tout cas une grande diversité d'actions du simple téléchargement illégal à la pédopornographie, sans oublier le phénomène complexe du darknet, à savoir ce réseau superposé (ou réseau *overlay*) qui, grâce à des protocoles spécifiques, permet des transactions illégales qui échappent au contrôle des polices. Bien entendu, aussi bien la protection de l'outil informatique que l'arsenal juridique à constituer doivent tenir compte de la diversité des actes commis. Ainsi un ordinateur peut être l'instrument d'un forfait, ou au contraire la cible. Le développement de la cybercriminalité implique une série continue de malversations s'en prenant de façon systématique à des sites ou transformant de façon tout aussi systématique l'instrument numérique en nouvelle arme au service du crime. Parmi les exactions qui se diffusent assez largement, il nous faut signaler la prédation contre les enfants, l'extorsion de fonds, le chantage, la manipulation des marchés boursiers, l'espionnage industriel de haut niveau, ainsi que la planification ou l'exécution d'activités terroristes. Il est à noter que le développement des moyens de lutte contre la cybercriminalité par les états fait sans doute dans l'immédiat reculer cette cybercriminalité, mais – et cela est singulièrement inquiétant – qu'elle trouve alors une nouvelle parade pour perpétrer ses exactions, souvent à plus large échelle et avec des conséquences plus graves.

22 La cybercriminalité se présente comme un défi majeur mettant du reste en cause une confiance peut être naïve en la neutralité d'internet qui serait une sorte d'espace vierge et sans inflexion particulière. Il est évident que le réseau par la façon même dont il est constitué suit une certaine codification qui l'oriente dans un certain. Et la cybercriminalité constitue alors une sorte de détournement de cette codification, bien entendu dans des buts illégaux. Lutter contre la cybercriminalité ne se réduit certainement pas colmater des brèches ou à réparer des dégâts

mais implique une prise de conscience, celle de l'évolution constante du cyberespace dans son ensemble et dans ses composants de sorte qu'il ne faut pas simplement mais contribuer à sa réinvention et à son amélioration constante au fil, du reste, des nouvelles menaces et des nouveaux défis. Bien entendu, d'une certaine façon le cyberespace nous semble pouvoir être compris comme un système adaptatif complexe. De même que l'on parle de virus informatique, il nous semble qie l'on pourrait parler d'une sorte d'homéostasie au niveau de chacun des cyberespaces et de l'ensemble des cyberspaces de même qu'une attaque serait comme une blessure physique ou une maladie. La question de la cybercriminalité dépasse les failles isolées car c'est le tout d'une certaine façon qui doit sans arrêt se reconstituer et trouver une nouvelle harmonie de fonctionnement. Ce tout est évidemment en lien permanent avec toutes sortes d'enjeux mais aussi avec des politiques menées à tous les niveaux, nationaux et internationaux.

23 L'inventaire de l'existant émirien constitue en tout cas un préalable indispensable pour mieux situer l'impact du numérique, présent et futur dans ce pays. La géographie physique d'un espace en très large part désertique, connaissant par ailleurs une forte concentration littorale, mais également avec un climat dominé par l'aridité, détermine une économie d'un genre particulier et un commerce ouvert sur les autres pays, grâce surtout à l'importance de son pôle littoral. L'atout pétrolier, qui peut aussi constituer une faiblesse dans la mesure où le pays se reposerait avec trop de confiance sur lui, manquant de diversifier ses sources de revenu, oriente forcément la politique internationale du pays. Il est vrai que malgré la séduction de l'atout pétrolier, les Emirats se sont toujours gardés de cette tentation, contrairement, en partie, au puissant voisin saoudien qui risque de devenir ainsi, un jour, un géant aux pieds d'argile. Enfin, et ce point nous semble justifier une attention toute particulière, les EAU, surtout en raison de leur histoire, constituent le seul état fédéral de la péninsule arabique. Il nous faut ainsi nous interroger sur le lien entre fédéralisme et démocratisation, grâce au numérique, peut-être dans un double lien de cause à effet. En nous demandant aussi dans quelle mesure le numérique ne favorise pas le fédéralisme, ou au contraire si le numérique n'induit pas un risque de centralisation, celle-ci étant rendue plus aisée, tout comme, même, le contrôle de la périphérie par un pouvoir central. A moins que la révolution numérique ne demande, pour être orientée de façon bénéfique, une véritable vision politique et institutionnelle qui lui donne son sens, et qu'elle ne commande pas à elle seule. Il y également lieu de se demander si les évolutions ne se font pas de façon paradoxale, autrement dit si une cause ne peut pas provoquer en même temps des effets contrastés ou opposés, et ce en proportions variables. Ainsi, la numérisation pourrait favoriser en même la centralisation et la décentralisation, ce qui pourrait conduire à une somme nulle à

l'arrivée, ou bien à ce que l'une des deux tendances se renforce au détriment de l'autre, même si ce n'est peut-être que provisoirement.

24 Or, notre recherche s'intéresse de façon spécifique à un pays, il faut ainsi connaître son histoire et son modèle politique actuel. Les Emirats, cet état indépendant n'existe comme tel que depuis une quarantaine d'années. Mais son émergence, si elle doit beaucoup sans aucun doute à l'influence britannique, qui s'inquiète forcément à ce qui peut se passer dans cet espace riche en pétrole, se comprend d'abord dans son cadre religieux et civilisationnel. Dès les premières années de l'Hégire, l'islam impose son hégémonie sur la région. Le défi qui s'impose donc à partir du VIIe siècle est celui de la conciliation entre une unité pacifiée et la diversité des tribus locales, caressant souvent des aspirations autonomistes. Des siècles plus tard, il semble que le modèle fédéral puisse contribuer à garantir un équilibre harmonieux. Aux VIIIe et au IXe siècles, sous la dynastie des Omeyyades puis des Abbassides, par exemple, tandis que la région connaît déjà un réel essor, à bien des titres, dont elle ne profite cependant guère, car il est surtout commercial et limité à ses côtes. Le bras de fer est constant entre les tribus et les puissances fédératrices. Plus tard, les Perses Bouyides puis les Turcs Seldjoukides tentent d'établir une domination à des fins aussi bien économiques que politiques. Des caravansérails comme Juméirah, l'actuel Dubaï, connaissent une prospérité croissante. Au XIVe siècle, la puissance émergente est le Royaume d'Ormuz qui contrôle de nombreuses îles et des littoraux. L'histoire des Emirats se poursuit dans le cadre international[14].

25 L'expansion coloniale, on le sait, marque une rupture autant qu'un nouvel élan[15]. En effet, le Portugal s'implante sur la côte Est du golfe d'Oman et prend Ormuz en 1507. A la même époque, l'Empire ottoman se présente comme son grand rival. Finalement, au bout de plus d'un siècle, les Portugais sont évincés, non sans avoir fortement réprimé les rebelles. En tout cas, à cette époque, les émirats actuels ne forment pas une entité spécifique mais font partie de la région dite "omanaise", avec une histoire somme toute commune. Les Ottomans et les grandes compagnies commerciales européennes se disputent le leadership alors que deux clans finissent

[14] Documentation historique très riche : Malcolm C. PECK, *Historical Dictionary of the Gulf Arab States,* Scarecrow Press, Lanham Md ; Eugen L. ROGAN, *Histoire des Arabes de 1500 à nos jours*, Paris, Tempus Perrin, 2016. Aussi : Alexis NORMAND, *Les émirats du golfe, au défi de l'ouverture*, Paris, L'Harmattan, 2011..

[15] A. H. de OLIVEIRA MARQUES, *Histoire du Portugal et de son empire colonial*, Paris, Karthala, 1998 ; André BOURGEY, « Histoire des Emirats arabes du Golfe » in *Hérodote*, 2009, 133, 2, 92-99.

par s'imposer : les Qawassim et les Béni Yas. Dubai se trouve au croisement de ces deux fortes influences. Au XIXe siècle, le Cheikh Zayed, dit le Grand, au long règne de plus de cinquante ans (1855-1909) donne l'avantage décisif aux Bénis Yas. Mais à cette époque, la présence britannique est de loin le plus déterminant.

26 Dès le début années 1820, Londres s'engage dans une coopération maritime et commerciale avec les chefs de la région, les cheikhs. Soucieux aussi de respecter les autonomies locales, le Royaume Uni reconnait également en 1835 son autonomie à Dubaï jusqu'alors unie à Abu Dhabi. Cet épisode est plus qu'anecdotique. L'équilibre du territoire, et donc sa vitalité économique, supposent à la fois une congruence mais également le respect des identités locales ne serait-ce que pour ne pas les exacerber en revendications autonomistes qui conduiraient à de graves tensions. La date de 1835 est particulièrement importante car une nouvelle trêve maritime est signée, destinée à être renouvelée, prodrome de futurs accords plus engageants. C'est en 1853, que ces trêves aboutissent à un traité de paix perpétuelle. La région est désormais mentionnée sous le titre des "Etats de la Trêve" ce qui annonce la situation actuelle. A l'époque, cependant, ce n'est pas le pétrole mais la perle qui représente la denrée la plus précieuse. Une différence particulièrement significative est l'absence de toute compétence de politique étrangère des "Etats de la Trêve". Cette dernière relève de ce qui est depuis 1876 l'Empire britannique. En ce sens, le statut d'état indépendant, reconnu au niveau international, des Emirats Arabes Unis, est totalement autre. Pourtant, les chefs des Etats, les cheikhs sont dès cette époque reconnus par Londres comme des partenaires économiques et politiques estimables. L'Angleterre reconnaît par exemple la demande du cheikh de Ras el Khaïmah d'être détaché de Charjah pour former un état autonome. En 1952, il en va de même de Foujeirah. A l'évidence, dans l'esprit de l'époque, la bonne harmonie de l'ensemble des Etats n'a rien à perdre d'une marge d'autonomie de chacun d'eux. Ce qui est exactement l'intuition fédérale. La même année 1952, un Conseil des Etats de la Trêve est établi. Prennent part aussi bien les cheikhs que représentants anglais. Les cheikhs, en effet, entendent bien garder leurs prérogatives et exercer leur responsabilité en matière de politique intérieure, au sein de leur Etat. Nous ne sommes pas encore dans le cadre d'un Etat fédéral mais d'une sorte de confédération au sein d'un protectorat. Outre les avantages traditionnels liés à la pêche et à la perle, les chefs des Etats bénéficient de plus en plus de rentes, en particulier liées aux hydrocarbures. Malgré une marge de manœuvre et de vraies compensations, la domination anglaise pèse de plus en plus lourd aux populations autochtones, alors que le monde dans son ensemble, suite aux deux guerres mondiales, et que

se répand de plus en plus l'idée du droit de chaque peuple et de chaque pays de disposer librement de lui-même. Par exemple, dès 1953 se met en place à Dubaï un front de rejet de l'emprise britannique. L'émergence de la Ligue Arabe, en soi assez peu efficace, mais surtout le sentiment d'une identité arabe [16] inquiètent Londres et plus largement l'Occident. Une crise éclate même en 1965, alors qu'un peu partout le colonialisme et même sa perpétuation sous un mode "soft" sont fortement contestés. Le cheikh Saqr Bin Sultan Al Qassimi de Charjah revendique une vraie autonomie, ce qui lui vaut d'être écarté et remplacé par un de ses proches moins intransigeants.

27 C'est la décision du gouvernement travailliste d'Harold Wilson en 1968 d'un retrait rapide de ses forces militaires se trouvant à l'Est de Suez qui ouvre en définitive la voie à une évolution longtemps préparée mais qui se réalise plus rapidement que prévue. Les Etats de la Trêve sont traversés par un double sentiment, pratiquement contradictoire. D'une part, ils ne peuvent que se réjouir d'un joug qui s'allège. Mais de l'autre, ils ne se sentent plus protégés, militairement, dans une région pourtant lourde de menaces. Car la présence britannique assure stabilité, sécurité, et une paix même relative. Les Etats de la Trêve se demandent alors ce qu'il adviendra d'eux, lorsque les garde-fous britanniques ne seront plus là, tandis que deux puissances voisines, plutôt antagonistes, l'Arabie Saoudite et l'Iran tentent d'avoir chacune le plus d'influence possible. L'idée est même avancée de payer à l'Angleterre le coût de son maintien dans la région, ce qui est significatif de l'importance de l'enjeu.

28 Selon le vieil adage, "l'union fait la force", les Britanniques conseillent vivement aux Etats de la Trêve, mais également au Qatar et au Bahreïn, de se fédérer pour pouvoir affronter différents risques. Un accord de principe est même signé entre les neuf souverains. D'autant plus qu'en 1971, la décision britannique de se retirer, est confirmée de façon décevante pour les Etats de la Trêve qui attendaient une politique différente du nouveau gouvernement conservateur d'Edward Heath. Malgré l'urgente nécessité d'un accord à trouver, les chefs arabes n'y parviennent pas. L'une des pommes de discorde est le lieu qui deviendrait la capitale du nouvel état. Al Khalifa, soulagé du renoncement de Téhéran à s'emparer de son pays, Bahreïn, en proclame l'indépendance et par là se retire du projet fédéral. Le chef du Qatar fait de même. Les Etats de la Trêve sont ainsi laissés à eux-mêmes.

[16] Robert MONTAGNE, "L'Union arabe", in *Politique étrangère*, 2, 1946, 179-195; Georges CORM, *Pensée et politique dans le monde arabe : contextes historiques et problématiques, XIXe-XXIe siècles*, Paris, La Découverte, 2015.

29 Six des sept Etats de la Trêve sont en tout d'accord pour créer un véritable état fédéral : le projet prend corps le 2 décembre 1971. Le septième état qui semblait hésiter, Ras el Khaïmah, ne tarde pas à les rejoindre dès le 10 février 1972. Il semble bien que les réticences de certains cheikhs aient été vaincues par la décision du souverain d'Abu Dhabi de placer une partie de ses revenus, qui tiennent aux réserves en pétrole de l'Emirat, au service de l'ensemble de l'Etat. Au demeurant ce cheikh Zayed bin sultan Al Nahyan devient alors le Premier Président des Emirats. Un nouvel état fédéral est né.

30 L'un des problèmes principaux affrontés par tous les pays est celui de la pesanteur et de l'inertie des bureaucraties en place, ralentissant les initiatives, voire parfois les rendant impossibles. La question n'est pas d'abord juridique au sens où des lois en vigueur feraient obstacle mais concerne des fonctionnements concrets. L'implication de nombreux intermédiaires fait courir le risque de résistances d'autant plus nombreuses. Dans les Emirats, en particulier à Abu Dhabi, les projets les plus visibles comme l'île des musées ou les centrales nucléaires tiennent leur succès d'une gouvernance directe se dispensant d'échelons intermédiaires, mais se dotant en revanche, grâce au numérique, de cabinets privés. Il y a lieu de parier que l'accroissement de la numérisation permettra encore davantage de semblables projets qui créent selon une expression souvent utilisée, des "poches d'efficience" qui sont structurées par des législations spécifiques, simples, souples et pragmatiques. Plusieurs exemples peuvent être donnés : les *free zones* de Dubaï ou encore une ville entière, Masdar, surnommée "la ville zéro carbone". Les *free zones,* qui correspondent plus ou moins à ce que l'on appelait des "villes franches" permettent des initiatives non soumises à trop de contrôles administratifs et connaissent une réglementation de l'emploi souple et attractive. La numérisation contribue encore à rendre rapides les processus décisionnels, déjà facilités. Enfin, dans ces *free zones*, des étrangers ont toute latitude de s'implanter et aussi de repartir, de sorte que les intérêts réciproques sont en général maximalisés. L'expertise étrangère mais aussi le volontarisme d'entrepreneurs venus d'ailleurs, relayés par le numérique, constituent un atout formidable. Il faut bien dire aussi que la richesse du pays permet d'éviter des conflits sociaux et la tension, sinon la paralysie, engendrée par des revendications syndicales difficiles à honorer ou tout simplement en contraste avec les impératifs de la modernisation d'une économie, comme c'est le cas souvent en France. Le numérique, sur fond d'une aisance économique globale, permet la régulation éventuelle de dissensions, rapidement et dans le sens d'un ajustement rapide des volontés des uns et des autres, en vue d'un profit maximal de tous.

31 Les Emirats ne bénéficient pas seulement d'une manne pétrolière exceptionnelle. Ils s'appuient sur leur position géographique pour remplir le rôle de pivot dans le contexte de la mondialisation. Cela est singulièrement vrai dans le cadre du transport aérien grâce à la construction d'infrastructures gigantesques même dans un rayon assez restreint. Par ailleurs, les Emirats investissent largement dans l'immobilier, mais ce filon efficace est compromis par la crise de 2008 faisant éclater la bulle immobilière. La construction dans le secteur public a repris le flambeau qui donne au pays des autoroutes, des écoles, des hôpitaux. Les potentialités des marchés financiers sont également très largement exploitées. Des critiques semblent souvent formulées accusant ces marchés d'opacité et le numérique peut constituer un remède à cet égard. Toujours est-il que Dubaï est souvent présentée comme le Las Vegas du Golfe. La vocation particulière de cette ville remonte sans doute au XXe siècle. La ville joue d'emblée la carte du libre-échange, déjà sous le cheik Maktoum, dès 1901, annonçant l'évolution à venir. Véritable capitale régionale depuis plus d'un demi-siècle, Dubaï connaît un nouvel essor au début des années 80 lorsque la guerre qui frappe le Liban empêche Beyrouth de remplir son rôle séculaire de porte d'entrée dans le Golfe. Grâce au cheik Rashid les grands axes du développement de Dubaï sont alors tracés. Son successeur, Maktoum bin Rashid a d'ailleurs repris le flambeau, avec un accent particulier sur l'infrastructure hôtelière. Le développement de Dubaï passe au demeurant par la création de zones franches aujourd'hui irriguées par le numérique. L'une des stratégies de Dubaï consiste dans la construction d'immeubles gigantesques, véritables prodiges architecturaux. C'est ainsi le cas des fameuses Tours des Emirats ou encore du Mall des Emirats, immense centre commercial. Outre Dubaï, les Emirats bénéficient de l'exception d'Abu Dhabi dont le territoire occupe 87% de la superficie d'ensemble, mais aussi, nous l'avons dit, trois quarts des ressources pétrolières, ce qui est considérable au niveau économique. C'est seulement en 2008 qu'après une longue réticence initiale Abu Dhabi opte opportunément pour la diversité économique, surmontant l'idée du "tout pétrole" pour accepter enfin l'idée d'investir dans des infrastructures. Abu Dhabi crée ainsi de nouveaux secteurs industriels en particulier grâce aux nouvelles technologies mais se consacre aussi largement aux énergies renouvelables, notamment solaires.

32 L'un des investissements les plus remarqués et les plus gratifiants des Emirats est dans le champ culturel. Le monde entier connaît l'émission télévisée *"Poet's Millions"* avec environ 70 millions de téléspectateurs. Une autorité culturelle a été créée à Abu Dhabi en 2005, l'ADACH qui ne se limite pas du tout à la valorisation de la culture régionale mais se veut un creuset et

un espace de rencontre entre cultures du monde entier, à l'instar de ce qui est censé se réaliser dans toutes les grandes métropoles du monde. Un quartier culturel se construit actuellement à Abu Dhabi dans le but d'accueillir des œuvres du Louvre ou du Guggenheim de New York. La constitution d'un musée de la mer et d'un musée historique national complète et diversifie cette offre culturelle. Les Emirats intègrent aussi à leur pratique des sports comme le football, très populaire, d'origine étrangère lointaine sans oublier pour autant leurs traditions comme les courses de voiles et de chameaux ou même l'équivalent du golf comme marqueur social, à savoir la chasse au faucon. Le touriste est frappé par l'importance - et l'élégance - des infrastructures sportives comme la célèbre Zayed Sport City à Abu Dhabi ou la Khalifa Sports City de Doha. Pour la première fois, en 2001, un grand prix de Formule 1 a été accueilli en 2009, à Abu Dhabi.

33 Les Emirats sont bien entendu pénalisés par le contraste entre le développement de la démographie et l'absence ou l'épuisement des ressources, en dépendance étroite avec la géographie physique. La pénurie d'eau reste une source permanente d'inquiétude. Mais à ce problème récurrent s'ajoute la pollution, également causée par les stations de dessalement, indispensables pour alimenter en eau plus de la moitié de la population émirienne mais induisant de nombreux dégâts collatéraux pour l'écologie. Par ailleurs, pour des raisons économiques, ce sont souvent les secteurs les plus polluants qui sont cultivés comme l'aluminium. La généralisation de la climatisation, compréhensible en regard du climat et des températures élevées, mais dommageable, constitue également un facteur hautement aggravant. Quant à l'essence, évidemment à bas prix, elle représente une des causes graves de la pollution. En positif, il faut saluer une prise de conscience progressive, bien que trop récente, de l'urgence d'une politique écologique vraiment drastique. La consommation d'électricité toujours croissante invite les Emirats à diversifier les sources d'énergie, par exemple en s'intéressant à l'énergie solaire. Nous avons déjà évoqué le projet original et prometteur de Masdar, cette ville dite "zéro carbone". La communauté internationale reconnaît en tout cas de plus en plus la bonne foi des Emirats comme en témoigne l'installation à Abu Dhabi en juin 2009 du siège de l'IRENA, l'agence internationale pour les énergies renouvelables dont la mission est d'assurer la transition vers ces dernières. Cette agence regroupe 149 états membres, ce qui laisse augurer d'une vraie crédibilité des Emirats quant à la transition vers des énergies non renouvelables. Ils entendent en particulier favoriser les énergies décarbonisées et réduire ainsi le recours au gaz naturel, énergie fossile largement explorée pour produire de l'électricité mais qui cause trop d'émissions de CO2 dont on sait l'impact sur le réchauffement climatique. Le recours au

nucléaire, rendu urgent dans les Emirats par le développement urbain, représente un point plus controversé. Pour le justifier il est fait référence à la croissance de la demande en électricité. En 2009, les Emirats ont signé un important contrat de 20,4 milliards de dollars avec un consortium privé pour intensifier le nucléaire.

34 C'est en tout état de cause dans la deuxième moitié du XIXe siècle que les Emirats, bénéficiant des revenus de la perle, commencent à investir dans l'éducation. Toutefois la crise économique de 1929 les incite à privilégier d'autres priorités. C'est la richesse obtenue grâce au pétrole qui redonne à l'impératif éducatif son importance. Si le Koweït est le premier dans la région à donner l'exemple, les Emirats s'investissent dans un rattrapage remarquable, notamment concernant les femmes et cultivent aussi des "économies du savoir", même si d'importants efforts demeurent à fournir en matière qualitative. Le renouveau de l'enseignement passe bien entendu par le numérique dont l'essor est rendu urgent par l'obsolescence et l'insuffisance de l'arsenal scolaire d'aujourd'hui. Les Emirats fournissent aujourd'hui un grand effort pour un meilleur enseignement supérieur. On peut citer l'Institut de Science et de Technologie de Masdar qui se trouve à Abu Dhabi et qui bénéficie beaucoup des développements du numérique.

35 La situation géographique des Emirats les pousse à souhaiter la protection des Etats-Unis pour conjurer d'éventuelles menaces iraniennes, irakiennes ou saoudiennes. La proximité d'un croissant chiite renforcé aggrave le sentiment de danger. Elle incite aussi les Emirats à s'affirmer sur la scène régionale, et par extension internationale, notamment au travers des médias, en assumant une distance politique et diplomatique renforcée vis-à-vis de l'Arabie saoudite, dont témoigne la rupture diplomatique de 2002. L'indépendance revendiquée par les Emirats en matière de politique internationale, ne les empêche au demeurant aucunement de participer, en fait de façon surtout symbolique, à l'opération occidentale en Libye. Mais il s'agit d'un engagement ponctuel et non de la sujétion à un camp. En fait, le numérique permet, et surtout permettra de plus en plus, aux Emirats de jouer de leur "soft power", pouvoir d'influence et de persuasion, théorisé on le sait par Joseph S. Nye, théoricien américain reconnu des relations internationale[17]. La stabilité et le rayonnement des Emirats, complétés par une efficacité renforcée dans leurs initiatives, font d'eux de véritables ponts entre le monde arabe et le monde

[17] Joseph Samuel NYE*, Soft Power. The Means to Success in Word Politics,* New York, PublicAffairs, 2004.

occidental et donc une charnière dans le cadre de la mondialisation, dans tous les secteurs, y compris culturel par l'architecture. Les Emirats peuvent donc se trouver plus facilement au cœur du numérique.

36 Il va sans dire qu'au-delà et en amont même des problèmes politiques et juridiques posés par la révolution numérique, celle-ci induit en effet une mutation d'ordre économique qui n'en est qu'à ses débuts, et qui doit aussi faire face à l'horizon de l' « après-pétrole »[18]. Comme nous l'avons dit plus, au départ, les Emirats se constituaient en réalité de petits états traditionnels dépendant, pour leur survie économique, d'une part, des relations commerciales avec d'autres pays, et d'autre part de la pêche des perles. Malgré certains signes d'essoufflement en partie liés à la complexité des fluctuations du marché, les Emirats ont connu globalement une bonne année 2019 incitant à un certain optimisme. Cela vaut en particulier pour le secteur des hydrocarbures qui a connu une hausse inespérée de plus de 7, 5%. La découverte de deux nouveaux champs de gaz, à Sharjah et à Jebel Ali constitue en outre un grand signe d'espoir pour le futur dont il convient de se réjouir. Mais ce dynamisme traverse aussi d'autres secteurs comme la banque, le tourisme, et la construction qui ont été d'autres points forts de l'année. Le lancement de l'expo 2020 marque également un moment fort de l'année 2020. Le bel élan espéré s'est hélas fracassé » sur l'affreuse pandémie du coronavirus, introduisant une récession entre 5 et 7 %. . Sans doute, l'économie émirienne ne sera pas à terre, mais néanmoins ébranlée et fragilisée. Il faut cependant espérer un rebond en 2021. L'impact du choc de la Covid19 pourrait heureusement être limité par le fait que le pays continue à disposer de larges réserves financières, de sorte que les comptes extérieurs devraient rester excédentaires malgré la baisse des prix des hydrocarbures. Ainsi, les Emirats devraient être le seul pays du Golfe à maintenir un excédent courant en 2020 et ce malgré la baisse des prix des hydrocarbures. Il faut rappeler à cet égard que le secteur bancaire des Emirats a opéré en 2017 un renforcement de ses activités grâce à des fusions bancaires. De plus les banques émiriennes sont aussi parvenues à renforcer leur présence sur d'autres marchés régionaux.

37 A l'évidence, la découverte des réserves en hydrocarbures, vraiment considérables, a entraîné une mutation totale et un envol, au début exponentiel. Depuis le début de l'exploitation

[18] Gilbert BASTIEN, Axel MARAUT et Benjamin TELLE*, Enjeux et perspectives pour les Emirats arabes unis. Et, après le pétrole,* Paris, Le Harmattan, 2005.

pétrolière en 1962 s'est ajouté la mise en valeur du gaz naturel. Aujourd'hui, les Emirats sont le deuxième producteur de pétrole du Moyen Orient, mais loin derrière l'Arabie Saoudite, très liée aux Etats Unis. C'est cette explosion économique due au pétrole qui est à l'origine de la modernisation si rapide du pays, de son économie, et de l'ensemble de ses infrastructures. Du reste, Dubaï abrite aujourd'hui l'une des plus grandes fonderies d'aluminium du monde. Il faut reconnaître que les Emirats ont été très chanceux de bénéficier de telles réserves de pétrole et de gaz. Ils ont su anticiper le monde d'après le pétrole, beaucoup plus que l'Arabie saoudite. Ils sont conscients depuis longtemps du danger de lier essentiellement la vitalité économique à un seul secteur et donc de la nécessité d'opérer une diversification. Actuellement, l'émirat d'Abu Dhabi, tente de suivre un plan à l'horizon de 2030. L'un des axes cultivés pour l'avenir par les Emirats est celui de l'économie du savoir, incluant bien entendu le numérique et l'intelligence, sans oublier des filons déjà bien cultivés comme l'aluminium, la céramique, ou encore les produits pharmaceutiques. 2009 est certainement une année à marquer d'une pierre blanche. Elle voit en effet l'annonce de l'acquisition par l'Advanced Technology Investment *Company* (ATIC) d'Abu Dhabi de *Chartered Semiconductor Manufacturing*, car il s'agit de l'un des plus grands géants de la puce électronique du monde entier. Les Emirats progressent beaucoup dans le développement de l'aérospatial. Même dans un émirat comme Fujaïrah l'innovation règne. On y lance en effet la première zone franche virtuelle des Emirats, à savoir un espace au sein duquel les compagnies détenues par des sociétés internationales peuvent exercer les activités commerciales à un coût moins élevé que dans les zones classiques, et ce à partir de n'importe quel lieu des Emirats. Un partenariat avec la Chine se développe en particulier dans le secteur du numérique. L'objectif est en effet d'explorer de nouvelles opportunités en lien étroit avec les grands leaders de l'industrie. Les deux puissances économiques cultivent l'idée d'une gouvernance numérique par le biais d'une plate-forme, gouvernance aussi qu'efficace. Bien entendu, pour des raisons conjoncturelles assez évidentes, le commerce entre les Emirats et la Chine a subi un ralentissement en 2020. Mais ce n'est recul temporaire qui permettra de repartir ensuite d'un nouveau pied sur le chemin d'une émulation réciproque et d'une croissance mutuelle. De fait, les Emirats sont bel et bien – et ce de plus en plus – le partenaire commercial majoritaire de la Chine. La nouvelle exposition numérique et commerciale, mise au point avec soin, se présente comme une formidable plaque tournante pour le futur.

38 Comment oublier la ville nouvelle de Masdar, une écoville et accueillant de très nombreuses sociétés spécialisées dans les énergies propres, tout en développant de façon remarquable la technologie des cellules photovoltaïques en couche mince grâce un certain nombre d'usines aux moyens ultrasophistiqués ? Masdar se situe aux Emirats Arabes Unis, plus précisément dans l'Emirat d'Abu Dhabi. Elle a pour ambition d'être une ville intelligente et verte. Le nom de la ville est déjà, à lui seul, tout un programme : il veut dire « source ».Sa construction n'a cependant commencé qu'en 2008. Le but du projet est de créer une ville intelligente et en adéquation avec la résolution des problèmes climatiques du pays. L'intention dominante est de substituer à une économie linéaire qui part de l'extraction et de la production pour finir avec les déchets à une économie de recyclage permanente, du moins autant que possible. Du reste, c'est pour cette raison qu'elle a été construite pour une vie « zéro carbone et zéro déchet ». Le défi est redoutable car la situation géographique et climatique de cette ville n'est en effet pas très favorable. La chaleur caniculaire et la sécheresse désertique ne contribuent pas vraiment à l'établissement d'une ville agréable à vivre. D'un point de vue écologique et en considération de la protection de l'environnement, la gestion d'une ville dans de telles conditions est en effet singulièrement improbable, d'autant plus que la climation à outrance est une grande consommatrice d'eau. L'usage massif du plomb dans l'essence et l'absence d'une vraie recherche des énergies durables constituent un handicap supplémentaire. Et il est assez facile de comprendre qu'une telle recherche d'une diversification énergétique n'était évidemment pas encouragée en priorité dans un pays si riche en hydrocarbures. Masdar a pour but premier d'être intelligente et verte, c'est pourquoi plusieurs aménagements ont été mis en place pour être le plus écologique possible. Un détail, mais qui a son importance : les immeubles sont très serrés les uns par rapport aux autres dans l'idée de garder le plus d'ombre possible, ce qui est très précieux sous la chaleur accablante. L'architecture est également bien faite pour éviter au soleil de pénétrer dans les demeures. Par ailleurs, la ville est aussi parsemée de nombreux panneaux solaires afin d'en tirer une électricité utile et même pour de nombreux usages. Même les lampadaires de la ville bénéficient chacun d'un panneau solaire destiné à l'alimenter. Tout se fait à pied – ou presque – dans cette ville qui inspire bien des urbanistes de par le monde entier, même s'il existe des voitures autonomes au service de qui doit se déplacer plus loin. Des voitures électriques bien entendu. Grâce à la mise en place d'un système très ingénieux d'aimants et de voies réservées, le système de Personal Rapid Transit (PRT) permet aux usagers de bénéficier d'une grande mobilité et de se déplacer très vite…et aussi de façon très écologique. Ce souci de l'environnement et de la mise en place très rapide d'une ville propre malgré une situation climatique et géographique défavorisée constitue d'ores et déjà un bon

point, et même un point excellent pour les Emirats, sur lequel il nous faudra revenir ultérieurement. Plus en détail.

39 Le secteur financier est toujours très dynamique dans les Emirats. Quant au tourisme, il justifie et suscite des projets qui sont, on le sait, pharaonique comme le célèbre hôtel Burj-Al-Arab. Hormis le cas singulièrement intéressant et passionnant des zones franches, le capital doit toujours revenir en majorité à des citoyens des Emirats. Notable est également l'investissement dans le secteur de la culture et des arts, comme en témoignent, de notoriété internationale, le louvre Abu Dhabi ainsi que l'exceptionnel parc des musées de la même ville, incluant le plus grand musée Guggenheim du monde. Le secteur de l'emploi, aux Emirats, est assez singulier : en effet, la population active compte une très forte majorité de non-émiriens, en particulier dans le secteur privé. Pour lutter contre un phénomène qui tend à s'accroître, est mise en œuvre une politique d'« émirisation » autrement dit de soutien aux Emiriens et en particulier dans le secteur privé, afin que les citoyens du pays redeviennent au moins un peu plus nombreux parmi les employés.

40 Depuis une vingtaine d'années, le commerce n'a cessé de se développer, en particulier avec le Japon, les Etats Unis et l'Union Européenne. La hausse des revenus du commerce, déjà dynamique, ne tient pas seulement aux hydrocarbures mais à l'ensemble des productions des Emirats, ce qui tend à confirmer l'observation faire plus haute d'une sage volonté de ne pas « mettre tous les œufs dans le même panier ». Parmi les éléments très prometteurs pour l'économie des Emirats, il faut encore relever l'ouverture de la capitale de Louis Dreyfus *Company* (LDC), géant du négoce de matières premières, aux fonds souverains d'Abu Dhabi, ainsi accueillis comme un investisseur et un partenaire de long terme. C'est la veuve de Louis Dreyfus, Margarita Louis-Dreyfus, une femme d'affaires suisse, qui est à l'origine de ce projet exemplaire et prometteur.

41 Aujourd'hui les Emirats sont au cœur de la transition numérique. Le pays entend exceller dans le domaine de l'intelligence artificielle et de la stratégie digitale pour s'imposer comme leader de ce marché dans une dizaine d'années. L'ambition avouée du pays est de passer d'une économie très centrée sur le pétrole à une économie de la tech. Un ministère de l'intelligence artificielle a d'ores et déjà vu le jour. Un conseil national de l'intelligence artificielle a été mis

en place et la recherche se centre aussi sur la blockchain. L'intelligence artificielle est mise en application dès les petites classes. L'adaptation concerne toutes les classes d'âge même si c'est de façon différenciée. Par ailleurs, les Emirats ont signé un partenariat récent avec la France et ont annoncé un investissement d'un milliard d'euros vers des sociétés françaises innovantes. Du reste, le pays envisage également de rejoindre le groupe international d'experts en intelligence artificielle, un projet franco-canadien mettant en avant l'éthique. De façon transparente, bien qu'implicite, il s'agit bel et bien de contrer de grandes puissances comme la Chine et les Etats-Unis, ce qui n'empêche pas par ailleurs un partenariat commercial sino-émirien du reste, par ailleurs. Les secteurs les plus porteurs aux Emirats sont les objets connectés, les villes intelligentes et l'informatique. Un exemple, parmi d'autres : dans les Emirats 92% de foyers disposent d'une ligne internet fibre optique. Aussi, les Emirats sont-ils le deuxième pays le plus connecté au monde. Bien entendu, ce développement du numérique s'étend bien au-delà du marché numérique. Ainsi, l'émirat de Dubaï s'est-il doté dès 2014 de l'entité « Smart Dubaï », visant à en faire la ville la plus intelligente (et la plus heureuse) du monde entier. Une vaste ambition sans doute, mais dont la réalisation commence bel et bien à se dessiner. Des résultats semblent déjà perceptibles comme la création de quartiers intelligents (Dubai Design District, Dubai Silicon Oasis) et de 500 spots wifi, ou encore l'installation de compteurs et de réseaux intelligents pour la distribution de l'eau et l'électricité. Toujours dans une même volonté rapide d'innovation, Dubaï s'est doté d'une feuille de route relative à l'usage technologie blockchain au sein des entités publiques en octobre 2016. C'est un jeune secrétaire d'Etat à l'intelligence artificielle, Omar al Alama, qui n'a même pas trente ans qui s'occupe de valoriser et de dynamiser le secteur numérique des Emirats. Les initiatives en faveur des smart city ne cessent de se développer pour faire de Dubaï une exception dans le monde entier. Il nous paraît également intéressant de signaler a présence d'une vraie filière française dans le secteur technologie et numérique. Ainsi, la communauté de start-ups françaises qui se trouvent aux Emirats est-elle vraiment florissante, avec plus d'une trentaine d'entités identifiées, fédérées autour du « French Tech Hub Dubai UAE », labellisé en octobre 2016., et ce avec des spécialités bien différentes. Les deux grandes voies d'avenir sont bien entendu la formation et l'enseignement. Une école numérique, comptant un nombre croissant d'étudiants, a en effet été développée après des recherches approfondies et un examen des principales expériences d'apprentissage mondiales sur la façon de mettre en œuvre un écosystème d'apprentissage numérique avancé et complet. On peut encore signaler le recours aux nouvelles technologies dans le domaine de la sécurité, en particulier grâce au robot policier. Le film célèbre Robocop a sans doute montré les forces et les faiblesses du policier robot. En tout cas, il y a trois ans, le

robot policier des Emirats est bel et bien entré en fonction au sein des forces de l'ordre de Dubaï, à partir d'un humanoïde développé et équipé de l'intelligence artificielle. Il parle en plus langues et peut en effet s'adonner à plusieurs fonctions. Le ministre de la police émirien, Abdullah Bon Sulla a d'ores et déjà indiqué qu'il souhaitait qu'en 2030 les robots puissent constituent un quart des effectifs de police. Et ce n'est qu'un début.

42 Il nous semble que les Emirats sont particulièrement dotés d'une capacité de résilience après des épreuves et des reculs comme du reste c'est le cas actuellement de la crise sanitaire du coronavirus. On se souvient de l'impact de la crise financière de 2008 qui a beaucoup secoué la conjoncture mondiale et par ricochet les Emirats, notamment avec le départ de travailleurs venus de l'étranger parfois très qualifiés et en tout cas fort utile. Suite à cette épreuve, les Emirats ont su reconstituer leur économie et développer quatre grands axes porteurs : le renforcement de la stabilité financière et bancaire, l'introduction de stabilisateurs en ce qui concerne l'emploi, l'amélioration de la compétitivité et le renforcement de l'investissement privé. Leur intuition très juste a été de mener une stratégie sur plusieurs côtés et fronts. Mais il faut surtout souligner que tous ces axes passent par le numérique qui en multiplie les bienfaits et l'efficacité. En effet, le numérique convient singulièrement bien à l'articulation entre le rôle de sponsor joué par l'Etat dans les Emirats avec les initiatives privées, ce qui suppose non seulement des données précises et à jour partagées par les uns et par les autres mais une grande rapidité d'interaction. En ce sens la conception dynamique, non sclérosée mais surtout positive, comme d'un tremplin, de l'Etat dans les émirats trouve son répondant dans les atouts nombreux de la révolution numérique et stimule en retour cette dernière. La politique menée est constamment attentive aux indicateurs de développement, notamment publiés par la Banque Mondiale mais aussi par le WEF (World Economic Forum), fondation siégeant à Genève et se réunissant annuellement à Davos et créée par l'économiste Klaus Schwab en 1971. Cette fondation se fixe pour objectif de donner une évaluation annuelle de la compétitivité de 133 pays. Le numérique permet alors un ajustement rapide entre les politiques des Emirats et les préconisations des indicateurs.

43 Le développement des Emirats et les enjeux qui lui sont liés sont permis par trois gages d'ouverture sociale[19], qu'ils pourront à leur tour renforcer. Ces trois gages sont : la tolérance

[19] Alexis NORMAND*, Les Emirats dui Golfe, au défi de l'ouverture*, Paris, L'Harmattan, 2011.

religieuse, les mutations progressives d'une tradition intégrée et non reniée, et enfin l'immigration importante.

Sans doute en contre-position/sens avec l'Arabie saoudite, unifiée par le wahhabisme, les Emirats cultivent un certain pluralisme dans le respect de tous. Certes les populations nationales sont-elles majoritairement sunnites, à l'exception de Bahreïn, majoritairement chiite, ce qui n'était pas jadis sans poser de problème puisque la conquête de cet archipel par la tribu sunnite des Al Khalifa plaçait les chiites dans une position de sujétion. Après un apaisement de la situation sur fond de développement économique, la Révolution iranienne de 1981 crée une nouvelle tension, encore aggravée par des problèmes économiques et sociaux suite au tarissement relatif de la manne pétrolière. Néanmoins, fort heureusement, l'arrivée au pouvoir d'un Hamad II ouvert aux réformes sociales et soucieux d'un "vivre ensemble" entre tous laisse augurer une situation plus apaisée. Mais les sunnites acceptent très bien la cohabitation avec les minorités chiites. De plus, ils tolèrent les petites minorités chrétiennes, hindouistes ou bouddhistes. Cette tolérance de fait n'est pas un fait nouveau. Elle dérive en bonne part de l'absence de rivalité historique entre religions ou confessions concurrentes. Les conflits pour le pouvoir ne se doublaient pas historiquement d'une guerre religieuse. De plus, la géographie physique spécifique du pays impose depuis toujours un commerce principalement littoral qui ne peut que favoriser l'accueil des marchands de foi différente. Pour éviter toute dérive fondamentaliste ou fanatique, des directives hebdomadaires sont données de nos jours aux imams de toutes tendances par les autorités. La liberté religieuse est un droit et un fait, même si le prosélytisme est exclu pour des raisons évidentes de paix civile et sociale. Le seul fait que les Emirats autorisent jusqu'à l'ouverture de temples sikhs témoigne de la volonté d'une cohabitation sereine des religions, atout fort pour les Emirats. La religion juive est tout aussi bien acceptée et respectée. C'est d'ailleurs une citoyenne bahreïnie juive, Houda Nonoo, qui représente le pays aux Etats-Unis. Si la religion musulmane fleurit et se diffuse grâce aux nouveaux moyens de communication, sous des approches théologiques variées, cet ancrage religieux nullement contesté ne compromet en rien l'ouverture aux autres. On peut même parler d'un certain modèle de laïcité évidemment très différent de celui de notre hexagone français mais qui assure un "vivre-ensemble" qui peut faire songer à certains égards, *mutatis mutandis,* à la situation concordataire de notre Alsace-Moselle française. La numérisation permet à cet islam ouvert d'être mieux compris et connu, dans un moment délicat de l'histoire du monde où le terrorisme des uns risque injustement de jeter l'opprobre sur les autres. L'organisation du culte et de l'enseignement est favorisée par le numérique et devient encore plus transparent.

44 Le deuxième gage d'ouverture, bien entendu lié au premier, est offert par l'évolution progressive de sociétés traditionnelles qui se modernisent sans ne se renier ni adopter une posture schizophrène, à savoir la conjonction d'une certaine modernité de surface avec des archaïsmes cachés. Le risque existe sans doute d'un bouleversement des structures familiales suite à l'urbanisation et aux mutations du monde du travail. Nous avons déjà évoqué les dommages collatéraux de ce qui est tout de même en soi un bien, le développement très rapide, comme certains problèmes de santé tels l'obésité ou le diabète. Il est vrai aussi que les services sociaux favorisent forcément l'individualisme, puisqu'il n'y a plus autant besoin des autres, surtout de sa propre famille, pour faire face à certaines graves difficultés. En même temps, les femmes gagnent très vite un autre statut, associées davantage aux informations et aux décisions grâce à la révolution numérique mais également grâce à une scolarisation en hausse. L'inscription dans des réseaux sociaux ouvre les horizons de tous au-delà des cercles de proximité initiaux comme la famille ou le quartier. La révolution numérique joue donc là aussi un rôle.

45 Le troisième gage d'ouverture est très largement donné par l'immigration. Contrairement à des politiques protectionnistes et frileuses, rétives à accepter le libre marché, les Emirats ont toujours joué la carte de l'ouverture sur l'autre. Dans certaines villes comme Dubai, les expatriés forment une très grande majorité de la population grâce au statut du "kafalah" qui permet la confiance entre l'employé étranger et l'employeur autochtone. Ce statut étonne beaucoup les Français et appelle peut-être des correctifs mais il doit d'abord être compris comme susceptible de favoriser l'embauche rapide et sans trop de risques ni pour l'employé ni pour l'employeur, dans une logique pragmatique. Le système a d'abord été expérimenté au Koweït. Son principe est simple, celui du parrainage par une personne physique ou morale du lieu d'un travailleur venu de l'étranger. Concrètement, il suffit d'être embauché pour être accueilli aux Emirats et obtenir un permis de séjour. En contrepartie d'un accueil si facile, il est assez normal que le pays exige des protections juridiques et responsabilise aussi l'employeur. Les abus existent, sans nul doute. Mais le contrôle est favorisé grâce au numérique qui permet de rendre plus transparentes les conditions imposées par l'employeur qui doivent respecter l'employé (ce qui veut dire aussi lutter contre des entreprises fantômes réduisant le salarié en quasi esclavage) et éviter aussi des abus, par exemple que des employés aient un second travail. L'un des problèmes, déjà évoqués, est celui d'une tendance des citoyens du pays à s'orienter vers la fonction publique, des étrangers mieux préparés et mieux spécialisés investissant l'espace de

l'entreprise privée. Néanmoins, malgré les dérives et les inconvénients que le numérique doit permettre de limiter par le contrôle strict et la transparence, la forte immigration favorise une société plurielle caractérisée par une classe moyenne aisée et harmonieuse. Ainsi, sans renier leur foi musulmane majoritaire, ni l'essentiel de leur valeur, les personnes qui forment aujourd'hui les Emirats, cultivent des valeurs de mondialisation, d'ouverture et de progrès, en syntonie immédiate avec le numérique et entretenues par lui. A cet égard, les recherches du sociologue iranien Vali Nasr[20], montrent le cercle vertueux qui se dessine : l'entreprise favorise l'immigration; l'immigration favorise l'entreprise; le numérique favorise les deux et l'harmonisation des deux. Les Emirats en 2020 ne sont plus les Emirats d'il y a encore quelques années mais ils ne sont pas encore les Emirats. C'est un chemin qu'il nous faut baliser, certes pas de manière contraignante mais en tenant compte de la marche même des choses à laquelle participe, tout en l'intensifiant et en l'accélérant, la révolution numérique.

46 Le rôle géopolitique des Emirats se présente également comme de plus en plus important et marqué[21]. On sait combien le golfe arabo-persique est devenu depuis plusieurs décennies un pivot des initiatives et des stratégies internationales. Du reste, pendant des millénaires cet espace a été une voie de passage et forme une aire d'échanges, comme un pont entre les civilisations même si ce rôle s'est en quelque sorte affaibli au XXe siècle. Présentement, les Emirats doivent faire face à deux puissances régionales de taille : d'une part, le géant iranien sur la rive nord du Golfe et d'autre part l'Arabie saoudite au sud. Depuis sa création, au début des années 1970, le pays doit faire face à d'importants enjeux géopolitiques et s'imposer dans une région de turbulences et de menaces. Le grand défi pour les Emirats est de se constituer mais également de se garder une personnalité internationale solide et stable. Les problèmes pour sa sécurité ne manquent pas et les exigences ne cessent de s'additionner comme celle d'une fixation précise des frontières ou encore du contrôle d'une population à la fois plus nombreuse et plus diversifiée. Il faut aussi veiller à la maîtrise des flux de personnes et de marchandises dans ce qui devient un pôle secondaire de la mondialisation. Quant à la pression exercée par les deux voisins saoudiens et iraniens, évoquée plus haut, elle est constante mais elle tend à s'intensifier à certains moments.

---

[20] Vali NASR, *Forces of Fortune: The Rise of the New Muslim Middle Class and What It will Mean for Our World,* New York, Free Press, 2009.

[21] Philippe BOULANGER, « Les défis géopolitiques d'une nouvelle puissance régionale » in *Hérodote*, 2009 133, 2, 58-91 ; William GUERAICHE, *Géopolitique de Dubai et des Emirats arabes Unis*, Nancy, Arbre bleu éditions, 2014. Aussi Charles SAINT-PROT (dir.*), Géopolitique des Emirats Arabes Unis*, Paris, Karthala, 2019.

47 La modernisation et l'essor économique des Emirats très remarquables attirent bien entendu des convoitises et des jalousies et attisent parfois des rivalités intrinsèques. Les mutations de tous ordres sont accélérées. Le pays dispose en tout cas de très nombreux atouts pour s'élever au rang de puissance régionale comme une volontarisme aiguisé et une population jeune. On sait l'importance, pour l'histoire récente des Emirats de la venue au pouvoir en 1971 du Cheikh Zayed en 1971 qui en fait l'un des grands axes de rayonnement, y compris du point de vue l'aide au développement et de l'aile humanitaire. Ainsi, l'autorité émirienne du Croissant-Rouge, par exemple, participe à aider les pays en développement et à apporter une aide d'urgence aux pays et régions victimes de conflits ou de catastrophes naturelles, distribuant près de 500 millions de dollars. Avec prudence, recul et réflexion, les Emirats refusent de s'ingérer dans les affaires internes des autres pays. Ils tentent de trouver des solutions aux conflits géopolitiques avec les pays voisins. Ses liens avec les autres pays du Golfe, à savoir Bahrein, Oman, le Qatar ou l'Arabie saoudite sont en soi facilités la création en 1981 du Conseil de coopération du Golfe qui n'a pas seulement une vocation économique. Dans un premier temps, les relations avec l'Iran se sont également améliorées malgré une détérioration et une complication depuis la crise du nucléaire civil en 2005. Le pays essaie cependant de maintenir le plus possible un dialogue ouvert. Un exemple très significatif de ce volontarisme positif a été donné en 2008 par la rencontre entre le ministre des Affaires étrangères émirien, Abdullah bin Zayed al-Nayhan, et l'ambassadeur iranien Reza Asefi, juste après la venue du Président Bush. L'un des bons points des Emirats aux yeux de l'Iran est la dénonciation vigoureuse de la part des Emirats des attaques israéliennes et fait apporter un soutien politique, économique et humanitaire au Liban. On peut aussi citer, en très positif, le programme émirien, adopté à la suite du retrait israélien du Sud-Liban en 2000, qui vise à l'élimination des mines et munitions non explosées, autre geste apprécié de soutien politique envers le Liban. Les Emirats ont toujours répété leur conviction selon laquelle la sécurité, la paix et la stabilité de la région ainsi que la normalisation des relations entre tous les pays, passaient nécessairement par l'établissement et la vraie reconnaissance d'un véritable Etat palestinien. Les Emirats ont toujours soutenu avec courage et énergie le droit international contre le terrorisme, les organisations internationales comme l'ONU et fait preuve à cet égard d'une moralité exemplaire au niveau international. Bien entendu, cette politique de rayonnement régional, se heurte malgré ses atouts et ses bons fruits à un certain nombre de limites. A commencer par les rivalités entre les pays voisins, déjà évoquées, en particulier dans tous les domaines de prestige,

comme le luxe, la recherche de haut niveau ou l'enseignement supérieur de grande qualité, sans oublier la construction d'immenses aéroports de transits.

48 Comme les enjeux économiques, les enjeux géopolitiques changent et évoluent au fil des années. En partie, ils se greffent sur d'anciens conflits comme autour des îles Tomb et d'Abu Musa. La menace iranienne est devenue plus intense au fil des années. Suite au développement interne du pays des menaces de sécurité interne sont également apparus. Reste aussi en suspens, le contrôle de la voie maritime du détroit d'Ormuz mais également la frontière occidentale avec l'Arabie saoudite. Il est intéressant de noter qu'il s'agit souvent d'anciens conflits du reste liés à la géographie physique sur lesquels se sont greffés des enjeux plus récents. L'imbroglio juridique règne bien souvent avec l'Iran tandis qu'une flambée de tension est perceptible. A la dimension géostratégique s'ajoute évidemment la dimension proprement économique car en cas d'aggravation notable de la situation dans le détroit d'Ormuz il y aurait de graves répercussions pour l'économie des Emirats. Des incidents ont souvent lieu. L'un des plus célèbres se situe au début janvier 2008 lorsque cinq vedettes iraniennes avaient harcelé trois bâtiments de la marine américaine et avaient menacé de faire sauter l'un d'eux, qui plus est au moment du passage du président Bush dans le Golfe. La tension qui existe renforce le contrôle des frontières incluant une nouvelle politique globale à cet égard. Longtemps, dans de tels espaces, avec une géographie physique très singulière, les frontières sont peu marquées dans la mesure où le désert en fait plus ou moins fonction. Désormais, les risques imposent un renforcement et une plus forte délimitation des frontières, bien clôturée avec de hauts grillages. Des systèmes de détection et de surveillance permettent par ailleurs de contrôler tous les mouvements éventuels. Ces frontières renforcées ont encore un autre but que celui de se protéger de voisins potentiellement menaçant : il s'agit aussi de mieux contrôler l'immigration dans le sens d'une limitation, afin d'éviter des indésirables, trop nombreux, qui mettent en péril la sécurité interne. On sait par ailleurs que des filières existent qui faciliteraient le passage de travailleurs en situation irrégulière. La chasse aux illégaux ne cesse en tout cas de s'intensifier dans les Emirats, en passant par une multiplication des contrôle policiers et diverses autres mesures drastiques (par exemple visa de travail obligatoire).

49 Mais les difficultés n'ont pas qu'un seul impact négatif. Elles favorisent aussi à leur façon la coopération régionale, autre élément de la politique sécuritaire. On mesure l'importance de la création le 25 mai 1981 par l'Arabie saoudite, Bahrein, les Emirats, le Koweit, Oman et le Qatar

du conseil de coopération du Golfe. Ce dernier vise à coordonner les différentes politiques – notamment étrangères – des différents pays, au départ dans le contexte des menaces exercées par l'Iran depuis le renversement du Shah. De plus en plus, l'objectif s'élargit et se transforme de plus en plus en visée vigoureuse d'un développement économique commun. Le 1er janvier 2003, une union douanière peut ainsi prendre forme. Ce conseil comprend en tout cas une véritable structure de coopération rassemblant tous les Etats du Golfe à l'exception – bien entendu – de l'Iran. Par exemple, un Conseil des ministres, comprenant les ministres des Affaires étrangères, se réunit tous les trois mois pour présenter des propositions et superviser les travaux du Secrétariat général. On peut saluer les nombreuses réalisations d'ordre économiques et les facilités que se font les Etats allant d'un permis de conduire commun à l'acquiiition simplifiée de biens immobiliers. Dans la suite de cette dynamique, l'accord économique de 2001, qui prolonge et remplace la Convention économique de 1981, crée un cadre favorable par des stratégies et des institutions communes, aussi bien que par la réalisation commune d'infrastructures, par exemple dans le secteur de l'aviation.

50 Les menaces au sujet de l'environnement sont évidemment elles aussi considérables pour les Emirats, le Golfe et le monde entier. La consommation d'eau a beaucoup augmenté dans un pays marqué par la sécheresse et les déserts, elle se présente même comme l'une des plus élevées au monder. Cela tient en bonne part à un fort accroissement de la surface cultivée. Or, une large part de cette eau consommée vient des nappes phréatiques ce qui laisse peser de très lourdes menaces. Les plages sont souvent souillées par les déversements de déchets et d'eaux usées. Bien entendu, comme toujours, les Emirats font preuve de beaucoup d'énergie et de beaucoup de volonté pour remédier à cette situation inquiétante, y compris par la recherche de solutions très variées allant de nouveaux systèmes d'irrigation plus économiques et plus sécurisés au recyclage des eaux usées. La surexploitation de la nappe phréatique fait peser de lourdes menaces et suscite déjà des dommages collatéraux. Ainsi se rapproche de plus en plus le spectre d'un épuisement des réserves mais on constate d'ores et déjà une augmentation de la salinité des sols. Les usines de dessalement des eaux travaillent déjà à toute allure et à pleins tubes pour répondre déjà aux besoins de la consommation courante. Ces usines dessalent l'eau puis rejettent le sel dans la mer avec de très graves conséquences. En effet, la salinité de la mer provoque d'importants bouleversements du milieu naturel.

51 Mais il faut encore envisager la coopération militaire qui peut prendre la forme d'exercices militaires conjoints mais aussi de stratégies mises en place conjointement. Toujours est-il que depuis 1983, les forces armées des pays du CCG organisent des manœuvres communes baptisées « Bouclier de la péninsule ». Ils entendent ainsi nette sur pieds, et ce très concrètement, une « force de déploiement conjointe », même si pour le moment, il faut le reconnaître, l'attachement à la souveraineté de chaque État rend plus difficiles et plus improbables des projets de plus grande envergure. On peut, du reste, regretter que chaque pays continue à mener une politique d'armement à outrance sans véritable consultation des États voisins, avec un arsenal d'armement très disparate. Les divergences ne parviennent pas à être surmontées comme cela apparaît assez clairement lors du sommet de Riyad en décembre 1987. Les alliances militaires choisies par les différents pays sont en tout cas loin d'être identiques.

Pour en revenir de façon plus strict aux seuls Emirats, dès la conquête de leur indépendance ils commencent à conclure des accords de coopération militaire et de défense avec différentes puissances occidentales comme le Royaume-Uni, les Etats-Unis et la France, dans un contexte qui est encore celui de la guerre froide. La coopération avec la France, depuis un accord signé en 1977, est en effet à souligner, qui passe par l'ouverture d'une base interarmes française. Mais cette coopération est aussi le révélateur pour les Emirats de sa dépendance à l'endroit de la puissance militaire des pays occidentaux, notamment les équipements français. Les contrats d'armements se développent depuis les années 1990. Le 18 janvier 1995, un accord de défense secret est même conclu en la France et les Emirats.

52 Le rapport entre les Emirats et l'Iran ont souvent été marqué au sceau d'une froide inimitié et d'un mépris réciproque[22] mais au fil des années, la situation s'est encore détériorée. Surtout depuis l'accord de paix entre les Emirats et Israël en 2020 perçu par le géant perse comme une trahison. Récemment pourtant, sans que l'on ne puisse parler bien entendu d'un quelconque rapprochement, les Emirats ont condamné dimanche l'assassinat «odieux» de l'un des principaux scientifiques du programme nucléaire iranien, Mohsen Fakhrizadeh, appelant cependant à «la plus grande retenue» alors que Téhéran accuse Israël d'être derrière ce meurtre. Plus récemment, les autorités émiriennes ont arrêté plusieurs Iraniens à Dubaï et à Abu Dhabi, soupçonnés d'avoir planifié des attaques terroristes contre Israël, en partie à l'occasion du

[22] Mehdi SABOORI, « Les Emirats Arabes Unis et les Iraniens », in *Hérodote*, 2009, 2, 133, 166-179.

premier anniversaire de la mort du général iranien Qassem Soleimani, tué à Bagdad dans une attaque de drone revendiquée par les Etats-Unis en décembre 2019. Le contexte est donc singulièrement tendu, et traversé par la crainte d'une flambée terroriste.

53 L'année 2020 n'a pas seulement été marquée par le début de l'affreuse pandémie du coronavirus mais encore par le rapprochement entre les Emirats et Israël, ce dernier étant fort de son statut de grande puissance économique et politique dans la région, sinon de point d'entrée du monde occidental. Un accord de paix bilatéral entre les Emirats et Israël a en effet été signé le 13 août 2020. Jusque-là assez discret, le rapprochement entre deux pays, et deux univers civilisationnels bien différents malgré les convergences de modèle économique, devient plus notoire et même exemplaire dans un certain sens. Il marque en tout cas un véritable changement de paradigme dans la région. Les menaces nouvelles – ou du moins leur intensification – , en particulier venant d'Iran, du Qatar ou de Turquie, rapprochent les ennemis d'hier. Le rapprochement qui se dessine est également révélateur d'une mise en second plan de la question palestinienne qui a été pendant des années la principale ligne de fracture. L'effacement ou au moins la relativisation de cette ligne de fracture longtemps perçue comme incontournable, insurmontable et aussi surinfectée, débouche sur un début de reconnaissance d'Israël dans le monde arabe, véritable nouveauté. Ce rapprochement s'opère d'ailleurs dans un climat de relative froideur qui tranche avec d'autres épisodes passés comme celui des accords de Camp David de jadis. Il traduit aussi d'une certaine mesure la primauté du poids des intérêts économiques sur des inimitiés séculaires dans la mesure où les échanges commerciaux entre Israël et les Emirats s'élèvent à plus d'un milliard de dollars, par exemple dans le secteur énergétique. Mais les secteurs qui devraient bénéficier de cet accord sont bien entendu très nombreux, y compris la culture et le cinéma. Sans aucun doute, le secteur du renseignement et de la répression est-il un atout majeur d'Israël aux yeux de pays arabes qui doivent relever de lourds défis dans ce domaine.

54 Dans ce contexte de fortes tensions et de nombreuses menaces, l'Arabie saoudite et les Émirats se résignent à conserver entre eux un mariage de raison. Le partenariat sans chaleur mais hautement stratégique qui les unit pour le moment semble pouvoir et surtout devoir résister aux secousses du contexte actuel. Certes, en juillet 2020, les Emirats ont-ils annoncé réduire leur contingent au Yémen où ils combattent depuis 2015 aux côtés de l'Arabie saoudite afin d'y chasser les Houtis et de rétablir au pouvoir le gouvernement en exil de Mansour Hadi. Ce refroidissement temporaire a certainement des raisons variées comme le souci légitime des

Emirats de rapatrier leurs troupes si besoin ou de donner un signal de détente diplomatique. En tout cas, redoutant l'escalade avec l'Iran les Emirats veulent éviter de multiplier les *casus belli* qui pourraient y conduire. La sagesse d'un telle ligne de profil est bien compréhensible : si d'aventure, les relations se détérioraient gravement entre les Emirats et l'Iran cela pourrait conduire au départ rapide des Emirats de professionnels étrangers très qualifiés et de grandes entreprises, donc à un choc économique bien redoutable. Des attaques asymétriques menées par des milices inféodées à Téhéran pourraient rapidement entraîner des conséquences d'une extrême gravité pour les Emirats. C'est pourquoi, même si les Emirats ont un discours très dur vis-à-vis de la République islamique d'Iran, ils veulent éviter d'arriver – au moins trop vite – au point de rupture et entendent se montrer « plus pragmatiques et prêts à discuter » que le royaume wahhabite. En outre, concernant la situation au Yémen, les Emirats sont fatigués de cette guerre dans laquelle ils ont déjà payé un lourd tribut. Pour autant, ils n'entendent pas non plus trop s'éloigner de leur allié saoudien et mènent donc un jeu diplomatique tout en bascule et en équilibre, risqué mais le seul possible et opportun. Il y a cependant une différence nette dans l'angle de vue des Emirats par rapport à celui de l'Arabie saoudite. Les Emirats sont convaincus qu'il est nécessaire de mener un combat de fond dace à l'Iran contre l'extrémisme religieux. L'Arabie saoudite se limite à un conflit stratégique et territorial pour empêcher l'Iran d'établir une base stratégique à sa frontière sud. Les visées et les perspectives diffèrent donc entre ces deux pays. Il est non moins certain que les Emirats attendent et espèrent une modernisation et une libéralisation en Arabie saoudite. L'alliance de raison, qui dure, entre les Emirats et l'Arabie saoudite n'est donc pas franchement enthousiaste mais pragmatique et attentiste. Indispensable mais inconfortable. En tout cas, la situation géopolitique recommande et exige même le recours le plus large possible, et le plus rapide possible, à tous les moyens offerts par la révolution numérique.

55 Bien entendu les jugements critiques ne manquent pas concernant les Emirats[23]. L'un des volets des critiques pointe du doigt le manque de transparence démocratique, des décisions opaques et parfois peu lisibles mais justement nous établirons que le pays entend de plus en plus avancer dans cette voie. Un autre volet est celui de la fiscalité, à inscrire aussi dans le cadre contextuel d'une grande disparité fiscale dans le monde entier, qui de toute manière est propice à des équivoques. Il est vrai que les Emirats sont un pays nouveau et très désireux d'attirer les

[23] Michel TAUBE*, La face cachée des Emirats Arabes Unis, Paris, Midi, 2019.*

compétences et les investissements, ce qui implique des facilités à l'encontre des partenaire, et une porte bien ouverte aux multinationales et aux hommes d'affaires conduisant à un achat facilité de bien et à un placement intéressant d'argent dans les Emirats. Depuis quelques années, le gouvernement émirien travaille d'ailleurs avec beaucoup d'énergie pour maximaliser l'impact de mesures fiscales plus rigoureuses, dans la ligne de celles qui s'appliquent en Union Européenne, et ce dans un étroit esprit de collaboration. Comme pour l'ensemble des points abordés et étudiés dans notre recherche, les Emirats mettent tout en œuvre pour une amélioration quantitative et qualitative, même si cette amélioration se heurte forcément à des opacités, pour des raisons diverses, et aux aléas comme la crise de 2008 ou celle toute récente du coronavirus, épreuves qui en compromet la linéarité. Mais justement l'explosion et l'accélération de la révolution numérique doivent contribuer à une évolution dans un sens très mélioratif.

56 Notre thèse contient donc deux dimensions en quelque sorte, toujours inséparables. D'une part, un inventaire, une analyse, une évaluation de l'existant dont nous avons déjà dit combien il était en évolution constante et accélérée, et pour lequel il n'est pas toujours facile d'opérer un arrêt sur image. D'autre part, des préconisations pour le futur. Notre recherche se situe donc plus ou moins constamment à l'interface du droit public et du droit privé, sans négliger ni l'un, ni l'autre, et bien entendu sans les confondre mais en les articulant car finalement la révolution est aussi et d'abord cela, une mise en rapport facilitée entre différents éléments que l'on traitait davantage isolément de par le passé.

57 Dans un premier temps, après nous être demandé si, et surtout dans quelle mesure, le fédéralisme, que connaissent les Emirats, constitue ou non une chance pour la mise en place d'un état intelligent, il nous faut envisager dans la perspective du droit public la mise en cause des limites institutionnelles que le numérique semble induire. Sans aucun doute, la révolution numérique semble appeler en écho une meilleure différenciation des niveaux de compétence, afin d'éviter tout télescopage, mais également leur coopération. L'horizon visé demeure celui d'un fonctionnement plus démocratique, impliquant une vraie participation des citoyens, dans l'expression libre et la prise de décision. A cet égard, le numérique qui favorise globalement l'efficacité devrait aussi renforcer la politique étrangère du pays, sa cohérence et son impact. Dans un second temps, le droit privé doit s'inquiéter des menaces mais aussi des atouts du numérique pour les citoyens et les entreprises, sans s'aveugler sur le danger de manipulation

souvent mercantile des données mais également en posant les problèmes épineux de la protection du droit à la confidentialité et du contrôle incertain des réseaux sociaux. C'est la défense de l'humain qui s'impose comme la vocation du droit privé au-delà des critères d'efficience technologique et de rentabilité économique. Dans la prise en compte des grands enjeux du futur comme la défense de l'environnement et l'adoucissement de la concurrence et des rivalités.

58 L'ensemble de la production bibliographique sur les Emirats se partage entre, d'une part, un courant visant à justifier les politiques menées et d'autre part un ensemble de publications très critiques, relevant parfois du réquisitoire et se caractérisant toutes par un manque d'empathie à l'endroit des populations locales. Une enquête journalistique menée en 2010 et jouissant d'un large écho médiatique, relayée par Raymond Barrett [24] entend démystifier de façon critique, la réputation de Dubaï. En revanche, un reporter comme Jim Krane peut à la même époque cultiver une réelle objectivité sans s'aveugler pourtant sur les limites[25]. Il est intéressant de saluer la rigueur intellectuelle et l'effort de Christopher Davidson, l'un des meilleurs spécialistes de la question, l'un des plus prolifiques aussi qui a le mérite de situer le cas particulier des Emirats dans un contexte plus large, à savoir les tensions et les richesses du monde arabe mais aussi le développement de la mondialisation[26]. Ses travaux constituent pour nous un socle de départ à compléter par les nouveautés les plus récentes et les plus contemporaines liées à la mondialisation. Malgré tout, certaines des positions de Davidson elles-mêmes sont aléatoires, improbables et idéologiques comme celles relatives à la fin des régimes actuels dans le Golfe. Bien entendu, nous avons lu et travaillé de façon détaillée les études classiques désormais de Frauke Heard-Bey, solides et très argumentées, en particulier son ouvrage de référence de 1982[27]. Mais beaucoup de choses, pour ne pas dire plus, ont changé en une trentaine d'années. Dans le souci d'une bibliographie plus récente, les travaux de Wanda Krause sur l'évolution de

[24] Raymond BARRETT, *Dubai Dreams. Inside the Kingdom of Bling,* Yarmouth, Nicholas Brealey Publishing, 2010.
[25] Jim KRANE, *City of Gold. Dubaï and the Dream of Capitalism*, New York, St. Martins Press, 2009.
[26] Christopher DAVIDSON*, The United Arab Emirates. A Study in Survival*, Boulder, Lynne Renner Press, 2005; *Dubai. The Vulnerability of Success*, New York, Columbia University Press, 2008*; Persian Gulf and Pacific Asia. From Indifference to Interdependence*, New York, Columbia University Press, 2010; *After the Sheiks. The Coming Collapse of the Gulf Monarchies,* Londres, Hurst & Co., 2012.
[27] Frauke HERARD-BEY, *From the Trucial States to the United Arab Emirates*, New-York / Londres, Langmann, nouvelle édition 2004.

la condition féminine sont à remarquer[28]. Tout comme ceux de Pardis Mahdavi [29] ou de Neha [30]sur le phénomène migratoire, par exemple indien. D'une plus grande importance encore dans le cadre de notre étude, un livre remarqué et remarquable d'Ahmed Kanna [31]met en évidence l'habileté avec laquelle les Emirats ont pu surmonter la crise de 2008. La surinformation sur internet, mais souvent sur le mode de la redondance, laisse croire à un nombre important de curieux qu'ils connaissent Dubaï alors qu'ils ont tout simplement été influencés par la diffusion de clichés. Nous savons depuis au moins Platon que la vraie connaissance qui est aussi compréhension (*logos)* a peu à voir avec la simple opinion (*doxa*). C'est pourquoi une surinformation, lorsqu'elle n'est pas désinformation, peut en fait cacher un manque profond de compréhension. Il est vrai que les Emirats ont peut-être en cela une part de responsabilité indirecte car ils se sont servi de techniques de marketing – mais n'est-ce pas une stratégie légitime ? - pour donner une image positive et attractive de par le monde, ce qui a pu en définitive susciter de la défiance, des spéculations hardies et hasardeuses, ou le sentiment d'un pays à la Potemkine, à savoir donnant simplement une image de façade très clinquante pour mieux dissimuler en fait un état de fait moins glorieux, comme le fit en son temps le favori de la tsarine Catherine II, grâce à des figurants et à des décors. La première condition pour comprendre les Emirats est de surmonter des grilles de lecture trop occidentales. Ce qui rend d'autant plus complexe le problème des sources et de leur exploitation. Les autorités du pays tiennent à la confidentialité d'un certain nombre de données. Quant à la presse du pays, qui nous livre une quantité d'informations, il convient de faire le tri entre différents types de données, celles relevant davantage d'une forme de communication orientée, et celles plus factuelles. Mais la première sorte de données mérite aussi l'attention, moyennant une lecture critique, se refusant à prendre pour argent comptant tout ce qui s'y trouve. Contrairement à une idée reçue, le presse n'est pas bridée et aborde des sujets délicats comme les affaires de corruption. Afin de mieux saisir de l'intérieur une situation, de mesurer les mentalités en présence, rien ne semble préférable à l'échange direct et de préférence oral et *in situ* avec des personnes partie prenante. En effet, l'échange direct s'il est relu et revu avec la distance critique que permet la prise en compte d'un coefficient de partialité parfois fort chez tout interlocuteur donne une perception plus vivante et plus stimulante des enjeux concrets.

---

[28] Wanda KRAUSE, *Women in Civil Society. The State, Islamism, and Networks in the UAE*, New York, Pelgrave Macmillan, 2008.
[29] Pardis MAHDAVI, *Gridlock, Labor, Migration and Human Trafficking in Dubai*, Palo Alto, Stanford University Press, 2011.
[30] Neha VORA, *Impossible Citizens. Dubai's Indian Diaspora*, Durham, Duke University Press, 2013.
[31] Ahmed KANNA, *Dubai. The City as Corporation*, Minneapolis, University of Minnesota Press, 2014.

59 Ces considérations méthodologiques expliquent sans doute pourquoi nous n'avons pas hésité, dans un premier temps, quitte peut-être à prendre un peu de retard sur l'échéancier personnel que nous nous étions fixé au départ, à consacrer tout le temps nécessaire à ce qui relève d'un patient travail d'investigation et ne saurait être remplacé ni par des lecture d'une bibliographie de seconde main étoffée mais répétitive et vite dépassée ni même par la simple consultation des documents officiels, justement en raison même de leur nature. Cet effort fourni, parfois un peu éprouvant, et rendu plus nécessaire encore par l'actualité mouvante du thème traité et de ses implications, nous osons espérer qu'il élargira notre vision des choses et rendra plus pertinentes nos suggestions. Comme on peut l'imaginer, nous avons passé des heures et des heures dans les bibliothèques en particulier celles de nos universités, mais également celle de l'Institut du monde arabe et comme il se doit la bibliothèque François Mitterrand, le site Richelieu-Louvois ne nous étant pas utile en raison du caractère contemporain de notre champ de recherche. Nous poursuivons notre enquête dans les différents espaces archivistiques y compris les archives de la diplomatie à Nantes ou bien entendu les archives nationales qui se trouvent à Pierrefitte-sur-Seine. En raison de la nature spécifique de notre recherche portant sur des phénomènes nouveaux et développement croissant et accéléré nous avons exploré aussi les librairies, notamment les rayons juridique et géographique, par exemple rue Soufflot à Paris. Affrontant également la difficulté du peu de sources ou d'ouvrages bibliographiques en langue française ou anglaise, nous obligeant à des allers-retours dans les Emirats.

60 L'état inchoatif de la législation et en bonne part de la pratique en ce qui concerne de façon plus spécifique les Emirats nous oblige à aborder les problèmes en quelque sorte de biais, en considérant la façon dont ils sont traités ailleurs, dans d'autres pays, et en particulier en France, mais également dans l'Union européenne comme telle ou aux Etats-Unis. Sans minimiser l'importance et la spécificité du contexte, on peut dire que les défis se posent souvent de manière analogue et qu'il est ainsi toujours fructueux et suggestif d'aller voir ailleurs ce qui est mis en place pour envisager de mettre en place d'autres mesures politiques et juridiques, une règlementation et jurisprudence. Cet état inchoatif de la législation émirienne et des stratégies déployées et à déployer nous incite donc à une étude bien circonstanciée même si quelquefois un peu cursive de l'histoire des politiques et des législations en la matière, telles qu'elles se présentent dans d'autres pays et qui peuvent ainsi inspirer, même *mutatis mutandis*, en fonction d'un contexte différent, les choix des Emirats.

61

En tout cas, en nous lançant dans ce travail de recherche, par attachement aussi à notre pays d'origine, c'est un double souci personnel qui nous maintient en haleine. D'une part, il nous semble que nous vivons dans une période extraordinaire d'essor technique et technologique, avec des opportunités qu'il faut absolument saisir au vol pour le bien de tous. Mais en même temps ce que suscitent l'intelligence et le travail de l'homme ne saurait devenir comme la « créature » du « Docteur Frankenstein » de Mary Shelley un monstre, faut-il doux, qui puisse lui échapper. C'est dans cette perspective que le droit public comme le droit privé nous semble prendre toute leur place pour humaniser et réguler un facteur décisif et en devenir constant de notre civilisation de demain. Nos constats et préconisations ne valent strictement que pour un pays, les EAU, mais de façon analogue peuvent également concerner les autres. C'est par le singulier d'une situation que l'on peut sans doute comprendre également les autres. Cette conviction anime en tout cas notre démarche.

62 Pour progresser dans notre recherche, nous privilégions deux étapes successives : Dans un premier temps, nous tentons à donner une vue panoramique de l'existant et de la situation telle qu'elle se présente aussi bien concernant les Emirats que les apports importants et parfois troublants du numérique. Nous nous efforçons en particulier de penser le cas particulier du numérique dans un Etat fédéral et d'être attentifs aux déplacements induits par cette révolution technique, en particulier dans la perspective d'une volonté de démocratisation qui est celle des Emirats. A l'évidence, le numérique permet plus d'efficacité et plus de transparence. Nous voyons ce que cela implique concrètement. Dans le contexte qui est celui d'une mondialisation croissante, et dans la mesure où l'essor numérique des Emirats est un peu plus tardif que dans d'autres pays, même si ce pays du Golfe tend à rattraper le retard, il faut aussi considérer avec attention ce qui se passe dans d'autres pays, notamment la France et les Etats-Unis. Dans un second temps, il nous semble essentiel – et complémentaire déjà – en fonction d'une étude du statu questionnais soigneusement établi en détails, de relever et d'évaluer combien et comment les Emirats relèvent déjà les défis mis en évidences dans la première partie, avant de nous risquer à des préconisations pour le futur. Dans cette perspective en particulier, il est très intéressant de faire référence aux réponses données par les autres pays, notamment les plus grands, aux problèmes analogues qui se posent. En tout cas, une attention toute spéciale est ensuite directement accordée à la cybercriminalité, à la cybersécurité et à la cyberdéfense. Notre recherche implique notamment une réflexion politique et philosophique mais entend se

positionner toutefois dans un cadre strictement juridique où il s'agit de peser avec équilibre les choix à faire, dans le contexte délicat et incertain d'une évolution constante qui s'accélère.

PARTIE I : LES DEFIS DU NUMERIQUE POUR LE MONDE ET LES EMIRATS

63 La révolution numérique n'a pas encore abouti à une sorte de point d'arrivée définitif dont il suffirait de dresser un panorama qui viserait à en suggérer l'état achevé. D'une part, elle se trouve dans un état encore inchoatif, en particulier pour les Emirats qui n'ont pas la même histoire, économique et politique, que les Etats-Unis et la France, et n'ont pas suivi les mêmes rythmes au même moment, ce qui ne veut nullement dire qu'ils soient condamnés à être toujours en retard sur l'évolution du monde. D'autre part, on peut raisonnablement se demander dans quelle mesure la révolution numérique, loin de n'être qu'une étape de changements importants en attendant une stabilisation, ne serait pas, en réalité, un processus constant de transformation, dans un monde plus liquide et plus volatile, qui loin de s'arrêter dans cette marche, la continuerait au fil des années et des décennies. C'est pourquoi, plutôt que d'introduire la fixité d'un point d'aboutissement, il nous semble plus judicieux de parler des défis et de les envisager dans une perspective continue et en partie imprévisible. Cette évolution n'est pas seulement, de façon abstraite, celle du monde entier, mais, indissociablement, dans un contexte de mondialisation, à la fois celle du tout et des parties, donc aussi de chaque partie prise en elle-même. Le monde bouge, car chacun des pays bouge en son sein, et vice et versa. L'approche doit donc être à la fois particulière et globale, spécifique et holiste, en raison d'une interaction constante que l'on peut aussi voir comme une causalité réciproque, dans les deux sens. Mais cela ne signifie en aucun cas qu'il ne faille, à cause de cette interaction constante, minimiser ce qu'il y a de spécifique à chacun de ses pays et qui oriente donc la façon singulière dont s'accomplit en lui la révolution numérique, et dont il est possible et opportun de l'accompagner et de l'encadrer, d'un double point de vue politique et juridique. Nous avons vu que l'une des caractéristiques les plus remarquables des Emirats, en regard notamment de pays proches qui l'entourent, réside justement dans le caractère fédéral de son fonctionnement institutionnel qu'il semble donc important de bien considérer comme tel.

TITRE I : LE MODELE FEDERAL FACE AU DEFI DU NUMERIQUE

Chapitre I : Le fédéralisme, obstacle ou chance pour l'Etat intelligent ?

64 Avant de préciser dans quelle mesure les Emirats sont non seulement en effet un état fédéral, mais surtout en quoi cette organisation particulière modifie la donne eu égard aux avancées du numérique, il convient au préalable de préciser qu'est-ce que c'est une organisation fédérale de l'Etat. Et ce d'autant plus que les Emirats Arabes Unis sont le seul Etat de la péninsule arabique à présenter cette singularité. Du reste, le fédéralisme ne se présente pas non plus de façon totalement univoque. D'autant plus également que certains états non officiellement de type fédéral (mais unitaires) peuvent en réalité avoir un fonctionnement fort décentralisé dans les faits, avec par exemple, comme en Italie, des échelons intermédiaires influents et déterminants. Soulignons cependant, d'emblée, qu'un état fédéral est un état souverain, pris en compte comme tel par le droit international. Pourtant, à la différence d'un état unitaire il regroupe plusieurs entités en partie autonomes, dans une mesure variable, en nombre variable et sous des appellations variables, jouissant parfois même d'une constitution, comme aux Etats-Unis, entités juridiques dont la nature et les contours restent toujours à définir et sont parfois en évolution. En tout cas, ces entités, quelle que soit leur marge d'autonomie, demeurent subordonnées à l'état fédéral lui-même, sans quoi il n'y aurait pas, en toute rigueur de terme, fédération mais confédération. Elles peuvent être multiculturelles et multiethniques. Néanmoins, la marge de manœuvre qu'elles conservent est significative d'une volonté d'équilibrer le pouvoir central et le pouvoir local et de respecter la compétence propre de chaque instance, qui ne saurait se voir privée de son droit légitime de traiter des questions de son ressort sans être court-circuitée par un échelon supérieur. C'est ce que le droit appelle le principe de subsidiarité [32] dont il est la forme concrète et diversifiée. Les Emirats sont en tout cas profondément marqués par leur héritage fédéral.

Section I : L'héritage politique à valoriser

65 Le fédéralisme n'est donc en rien un corps étranger qui aurait été importé par quelque décision dans les Emirats. Au contraire, il exprime un souci constant qui traverse toute l'histoire de cet

[32] Cf., entre autres, Jean-Louis CLERGERIE*, Le principe de subsidiarité*, Paris, Ellipses, col. ' le droit en question', 1997)

espace géographique. C'est pourquoi, notre recherche doit nécessairement inclure une présentation de l'histoire de la région de sorte que la situation actuelle puisse véritablement apparaître comme un aboutissement. Et ce d'autant plus que, sans contradictionavec le souci de grande modernité technologique et économique ni avec un rééquilibrage du fonctionnement du régime dans un sens plus démocratique, les Emirats restent attachés plus que jamais à leur tradition et veulent inventer le présent et le futur comme un développement homogène de celle-ci. En attendant, il nous paraît opportun et même indispensable de faire quelques rappels historiques et juridiques sur ce qu'est le fédéralisme, afin que les mots aient bien un sens.

a. L'essence du fédéralisme

66 Le fédéralisme n'est évidemment pas né dans le cadre de la Péninsule arabique, ni même aux Emirats, le seul pays actuel à l'avoir adopté et à le cultiver. Il constitue une forme de structuration d'un Etat élaboré et théorisé dans le monde occidental. Au départ du fédéralisme se trouve donc une conception philosophique, et même plus précisément, théologique, que l'on trouve déjà chez les Pères de l'Eglise chrétienne, développée et systématisée en particulier par le philosophe protestant Johannes Althusius [33](1557-1638) mais aussi de façon générale dans toute pensée politique et juridique inspirée du christianisme[34]. Ce principe est cependant repris, outre des théologiens comme Thomas d'Aquin[35], aussi bien par des penseurs de tendance socialiste comme Pierre-Joseph Proudhon[36], que par des libéraux anglo-saxons comme John Locke ou Stuart Mill. Sans aucun doute, l'idée de subsidiarité et partant celle de fédéralisme a émergé dans un contexte européen. Pour autant, cette intuition entend revêtir une dimension internationale, s'appliquer également à d'autres contextes et à d'autres cultures. Un principe peut évidemment être décliné de façon très diverse en fonction du contexte, des circonstances, des

[33] Cf. Gaëlle DEMELEMESTRE*, Introduction à la « Politica Methodice Digesta » de Johannes Althusius*, Paris, Ed. du Cerf, coll. 'Humanités', 2012.
[34] Cf. Julien BARROCHE, "La subsidiarité. Le principe et l'application", in *Etudes,* Paris, 2008, 6, 408, 777-788.
[35] Cf. Chantal DELSOL, *Le principe de subsidiarité*, Paris, PUF, col. 'Que Sais-je?', 1993 montre bien l'importance de ce principe aussi bien dans la théologie politique que dans la doctrine de l'Eglise et l'influence historique d'un Thomas d'Aquin.
[36] Pierre-Joseph PROUDHON*, Du principe fédératif et de la nécessité de reconstituer le parti de la révolution*, Paris, Romillat, 1863; Christian REVEILLARD, "Proudhon et le fédéralisme", in Jean-Pierre DESCHODT (dir.), *Pierre-Joseph Proudhon : l'ordre dans l'anarchie, Centre de recherches Hannah Arendt, Institut Catholique d'études supérieures*, Paris, Ed. Cujas, 2009, 135-157.

opportunités. Le fédéralisme [37]se présente d'abord, donc, en soi, comme une idée abstraite voire une vision utopique, mais il inspire la création d'état fédéraux. L'état fédéral se présente en tout cas comme l'expression volontaire au niveau d'un pays d'une volonté de déconcentration et de meilleure répartition des rôles et des fonctions. On peut le présenter comme un état souverain mais laissant à des entités de l'échelon subalterne les responsabilités qui leur incombe. Nous verrons que l'histoire singulière de l'espace géographique des Emirats, par une heureuse coïncidence, se prédispose à l'implantation d'un modèle fédéral.

67 Les limites entre Etat fédéral et Etat unitaire [38] sont cependant plus floues qu'une présentation schématique ne le laisse entendre. L'état unitaire lui-même qui se définit pourtant par la concentration en une seule instance ultime des compétences souveraines, n'exclut pas forcément la décentralisation et certaines formes d'autonomie subalterne. En effet, on trouve des Etats unitaires possédant des subdivisions territoriales, se gérant en partie elles-mêmes. Le cas le plus flagrant est celui de l'Espagne, état unitaire mais pourtant à certains égards présentant des traits d'ultra-fédéralisme [39] Ainsi, on peut légitimement se demander si la distinction opérée entre état unitaire et état fédéral n'est pas, quelquefois, assez formelle. En théorie, le premier n'accorde des espaces d'autonomie qu'en fonction de son libre vouloir. En revanche, le second est tenu de respecter ces mêmes espaces d'autonomie indépendamment de son bon vouloir. Le processus par lequel un état devient fédéral est celui d'un accord entre d'anciens états indépendants. Quant à l'autonomie des régions, elle est souvent créée au travers d'un mécanisme de dévolution. Il faut que l'Etat unitaire accepte d'accorder de l'autonomie à une partie de son territoire. Et cette autonomie, il peut toujours, sous certaines conditions, la lui retirer. On doit cependant reconnaître qu'il existe des états fédéraux de fait, non reconnus officiellement comme tels, mais qui accordent en définitive davantage d'autonomie à des entités régionales que de véritables états fédéraux ainsi nommés. Il y a parfois loin de la théorie à la pratique. C'est sans doute le cas déjà cité plus haut de l'Espagne qui concède à des régions comme la Navarre, la Catalogne, ou le Pays basque une autonomie beaucoup plus vaste. Certes, en théorie, cette autonomie n'est que concédée, donc révocable, mais dans les faits on peut dire qu'elle s'impose, car si le Parlement espagnol s'avisait, aujourd'hui, en tout cas, de la remettre en cause, il y aurait lieu de

[37] Cf. parmi une abondante bibliographie les deux ouvrages classiques : Bernard VOYENNE, *Histoire de l'idée fédéraliste,* Paris, Presses d'Europe, 1976; Bernard BARTHALAY, *Le fédéralisme*, Paris, PUF, 1981. Cf. aussi William H. RYKER*, Federalism : Origin, Operation, Significance*, Boston, Little Brown, 1964)

[38] Sur la distinction entre les deux il suffit de se référer à l'ensemble des traités de droit. A noter sur internet une dissertation très claire :
http://www.academia.edu/5602542/Droit_Constitutionnel_Etat_Unitaire_Etat_F%C3%A9d%C3%A9ral.

[39] Cf. Pierre SUBRA de BIEUSSES, "Un état unitaire ultra-fédéral" in *Pouvoirs*, Paris, 2008, 1, 124, 19-34.

craindre une crise politique majeure. On peut donc parler d'une quasi-impossibilité pratique de remise en cause d'une autonomie, même si cette dernière n'est pas coulée dans le marbre de la constitution. Par ailleurs, certaines régions de la péninsule ibérique disposent même d'un contrôle total sur la fiscalité ou le budget, et s'arrogent la part du lion ne versant qu'une somme réduite au gouvernement central. Dans le contexte international actuel, il est également intéressant de noter qu'une forme de fédération de fait s'est imposée en Chine. Les provinces disposent de grands pouvoirs, en particulier au plan économique. On parle quelquefois d' « un fédéralisme à la chinoise », pour des raisons fondamentalement économiques il est vrai, comme il a pu exister après Mao sous Deng Xiaoping un vrai « communisme à la chinoise ». Chacune des régions administratives bien spécifiques de la République populaire de Chine, dispose de compétences précises qui lui sont proches et qu'elle entend assumer pleinement[40]. C'est surtout en Suisse et aux Etats Unis que le fédéralisme a commencé à fleurir mais d'abord sous le modèle de la confédération, c'est-à-dire d'entités qui gardent pour l'essentiel leur pleine entité. Ce modèle est ainsi né des aléas de l'histoire et notamment du pacte défensif entre les cantons d'Uri, de Schwyz et d'Unterwald, en 1291, qui se trouve à l'origine du pays. En 1787, l'Etat fédéral, cette fois, au sens vrai et propre du terme apparaît avec la Constitution des Etats-Unis d'Amérique en 1787, qui succède à une confédération transitoire qui a duré dix ans de 1777 à 1787. Quant à la Suisse, elle adopte elle-même une constitution fédérale en 1848 de sorte que le titre de confédération helvétique ne convient pas véritablement. Elle forme à présent un véritable état fédéral. Outre ce modèle moderne d'état fédéral, il a existé dans l'histoire une forme de fédéralisme communautaire dans des Etats comme l'empire aztèque, l'Inde, la Chine ou la Turquie regroupant des communautés essentiellement définies par l'origine et la religion. Ainsi, se forment des regroupements interconfessionnels et interethniques. Suivant un tel modèle, chacune des communautés non seulement cultive sa propre religion et ses coutumes mais encore des statuts spécifiques, des législations particulières, par exemple familiales. Encore aujourd'hui, la prise en compte de telles communautés perdure sur ce modèle au Maroc, en Iran ou au Pakistan. L'une de ses expressions est que les communautés spécifiques disposent de sièges réservés au Parlement.

[40] XIAOHONG XIAO PLANES, "Constitutions et constitutionnalisme : les efforts pour bâtir un nouvel ordre politique" in Mireille DELMAS-MARTY et Pierre WILL*, La Chine et la démocratie*, Paris, Fayard, 2007, 259-294.

68 L'Etat fédéral est donc d'abord un modèle politique diversifié, dont le choix tient en général à un contexte et à une histoire qui rendent son adoption souhaitable. Ce modèle se caractérise par un certains nombres de principes dont le premier peut être nommé le principe de superposition, ou de répartition des compétences, de sorte que le gouvernement fédéral comme les états fédérés se divisent les compétences de façon équilibrée, sans exclusive ou prérogative excessive de la part de l'un ou de l'autre des niveaux. Toutefois, en général, le niveau fédéral l'emporte et chapeaute le niveau des entités fédérés. La Belgique constitue, au demeurant, une exception intéressante, car les entités fédérées ne sont pas contrôlées par l'état fédéral mais au même niveau que lui. On peut aussi parler d'un principe d'autonomie ou de subsidiarité, déjà évoqué plus haut, car d'une certaine manière il est la justification juridique et peut-être éthique du fédéralisme. Le niveau de l'entité fédérée ne doit pas se voir privé de son pouvoir de décision et une compétence qui lui incombe ne doit pas être en quelque sorte court-circuitée par une instance supérieure. A la base de ce principe se trouve la conviction d'un droit fondamental pour chacun, personne physique ou morale, de ne pas être privé de sa compétence propre. On peut encore évoquer un principe de participation : les entités fédérées sont représentées dans les instances fédérales et participent aux décisions fédérales prises. Au plan strictement constitutionnel, la confédération n'est pas un état. Les deux seuls régimes pour un Etat sont l'Etat unitaire et l'Etat fédéral. Ce qui n'empêche pas des confédérations initiales de devenir des Etats fédéraux, comme dans le cas évoqué plus haut des Etats-Unis et de la Suisse. Parfois aussi, en particulier dans l'histoire récente, certaines confédérations se divisent en états indépendants, c'est le cas de l'ancienne confédération de Sénégambie, entre le Sénégal et la Gambie, en 1972. La confédération comme la fédération présentent l'une et l'autre des avantages. La confédération garde une marge de liberté plus grande aux Etats confédérés. En revanche, une fédération donne la garantie de davantage d'efficacité et limite les blocages. En général, les pouvoirs dits régaliens, c'est à dire ce qui est lié à la souveraineté et qui appartient en propre à l'Etat, relèvent de l'Etat fédéral comme tel! Il s'agit en particulier des Affaires étrangères, de la Monnaie ou de la défense nationale. L'enseignement ou la culture relèvent plus souvent de la compétence de l'échelon fédéré.

69 Il est possible de postuler dès le départ que le fonctionnement d'un Etat tiendrait d'abord à son histoire, à la façon dont il s'est constitué. L'exemple des Etats-Unis est instructif à cet égard[41].

[41] Cf. le classique Gordon S. WOOD, *The Creation of the American Republic,* 1776-1787, Chapel Hill, NC, University of North Carolina Press, 2 éd., 1998.

Le fédéralisme américain naît d'abord de l'histoire. Lorsque la révolution éclate, le pays connaît déjà treize Etats indépendants, les premiers de l'histoire à bénéficier d'une constitution. Par la suite, pour les rassembler sans les priver de l'autonomie à laquelle ils demeurent attachés, il n'est pas possible de les priver de la constitution qui est propre à chacun d'eux. En revanche, il a été décidé de superposer une constitution supplémentaire, fédérale quant à elle, qui n'entrerait pas en conflit avec chacun des constitutions propres aux différents Etats mais régenterait un nouveau niveau de compétences. De la sorte a été établie une séparation des pouvoirs, encadrée qui plus est par une Cour constitutionnelle, la Cour Suprême chargée de vérifier qu'il n'y ait pas de conflit de compétences, et en particulier que l'autonomie de chacun des Etats soit préservée.

70 Après ces prolégomènes sur le fédéralisme comme tel et ses différentes incarnations institutionnelles et politiques il faut nous intéresser de façon spécifique à l'histoire des émirats pour comprendre en quoi justement le fédéralisme lui convient singulièrement bien, puisqu'il est en harmonie avec la trajectoire d'une longue construction d'un pays, sur fond de référence à d'anciennes traditions.

b. La tradition fédérale ante litteram d'une région

71 Dans les cas qui nous intéresse directement, celui des Emirats Arabes Unis, il faut rappeler que le pays n'existe comme tel que depuis 1971 et qu'il s'inspire du modèle des Etats de la Trêve[42], qui eux-mêmes s'inspirent largement d'une histoire plus ancienne encore, celle d'une cohabitation entre cheikhs. On le sait, c'est la défaite des Qawasim en 1819, ces marins, pêcheurs, et pirates, frappés par la flotte britannique lorsque la frégate HMS Liverpool tire sur Ras al-Khaimah qui marque ce qu'on appelle un véritable « Turing point » lorsque le Royaume-Uni décide de s'entendre avec chaque cheikh pour forme de confédération. Mais un détour historique s'impose pour comprendre en quoi ce tournant décisif s'inscrit cependant aussi dans une certaine continuité.

72 Dès les premières années de l'Hégire, l'islam impose son hégémonie sur la région. . Bien plus, il donne à cet espace sa cohésion et sa vitalité, « une impulsion qui lui permet de survivre à tous les échecs politiques, de durer jusqu'au seuil des temps modernes »[43]. Mais avant

[42] Cf. Donald HAWLEY, *The Trutial States*, Londres, Allen and Unwin, 1970.
[43] Jean-Paul ROUX, *Les Abbassides. Les legs culturels d'un empire éphémère*, Paris, Clio, 2001, 27.

73 même l'expansion et l'implantation de l'islam, les grandes décisions étaient nécessairement le fruit d'un consensus politique entre chefs de tribus, des cheikhs, en effet dotés d'un fort prestige personnel. Dès l'antiquité, en effet, l'Arabie est formée de tribus bien organisées commandés par des chefs. Aujourd'hui encore, d'ailleurs, d'une certaine façon, les Emirats peuvent s'appuyer sur cet héritage. L'autorité morale et spirituelle d'un leader s'impose comme un facteur de cohésion interne et de paix avec les autres. Le chef du clan est choisi en général sous le mode de consensus, même si l'hérédité constitue un facteur bien entendu très favorable quoique non exclusif : c'est souvent le fils aîné du chef défunt ou d'une grande figure qui est choisi. Le conseil de famille joue un rôle très important. Les notables du clan sont plus que de simples conseillers : de véritables autorités qui orientent les décisions et dont le chef ne peut court-circuiter les avis. De même, les autres chefs de clan doivent-ils avoir un droit de regard sur la politique qu'il mène à l'intérieur du sien, ce qui laisse à penser à un gouvernement de type plus collégial qu'autocratique mais engageant néanmoins la responsabilité personnelle. Le crédit moral du chef constitue un critère essentiel. Par la suite, une fois que ces tribus rejoignent l'islam, l'arbitraire du chef et de son conseil sont encore limités par le poids de la tradition, de la sunna. Mais l'homme contemporain ne peut manquer d'être agréablement surpris par une sorte de caractère « proto-démocratique » des prises de décision qui ne sera jamais renié. Un mérite d'un passé illustre qui éclaire et inspire aujourd'hui encore la politique des EAU et que l'historien Joseph Chelhod a su mettre en lumière. [44].

74 La première grande dynastie régnante est celle des Omeyyades. On connaît leur rôle de bâtisseurs. Mais aussi leur volonté d'expansion territoriale du monde arabe. Toujours est-il qu'ils posent les bases dynastiques du monde arabe cultivant les valeurs de l'aristocratie et de l'excellence. Ainsi le califat devient-il une autorité non seulement religieuse et spirituelle, mais aussi politique et juridique. On peut donc voir en cette période un premier âge d'or du nationalisme mémoire dont la mémoire constitue une référence importante. Se forme aussi, sous leur férule, une sorte de classe d'érudits et de savants qui se charge de l'historiographie et des chroniques. Toujours est-il que « sous les Omeyyades, les Arabes ont créé les conditions dans lesquelles une civilisation islamique a pu se développer dans les grands centres urbains du Proche Orient ancien »[45]. Bien le facteur religieux demeure important, mais l'impératif le plus

[44] Joseph CHELHOD*, L'Arabie du Sud, structures du sacré chez les Arabes,* Maisonneuve et Larose, 1984.
[45] Panayiotis Jerasimof VATIKIOTIS*, Islam and the State*, Routledge, 1987 ; tr.fr *: L'islam et l'Etat*, Paris, Gallimard, 1992, 24)

urgent est de stabiliser et de centraliser un univers trop chaotique. La cohésion sociale est assurée alors par la loyauté de tous envers un chef politique, en particulier face à la menace d'attaques extérieures. L'aristocratie arabe rachète les terres de propriétaires non arabes et s'impose comme privilégiée ce qui suscite des mouvements de population, en particulier des musulmans non arabes, originaires des territoires conquis, mais ayant rejoint l'Islam. On appelle ces derniers les *mawali*. Qui revendiquent une égalité réelle pour tous les musulmans ce qui n'est pas contradictoire avec la dhimmitude statut imposé aux non musulmans. Les dhimmis doivent d'ailleurs un lourd impôt. En raison d'ailleurs de l'importance pour lui de cet impôt, l'Etat ne fait aucun prosélytisme susceptible de diminuer le nombre des mawali, donc de ceux qui paient beaucoup moins d'impôt ! Mais cette réticence au prosélytisme tient aussi d'un vrai souci de la sincérité des conversions qui ne sauraient être motivées par une simple volonté d'éviter l'impôt. Le fossé tend hélas à se creuser entre les mawalis et les musulmans arabes, les premiers ralliant massivement le chiisme. La tension finit par aboutir à une révolte mawalie en 685, écrasée violemment. Mais la fronde des mawalis persiste de façon souterraine et pourtant efficace. Finalement, un courant chiite, celui des Hachimiyya finit par déstabiliser le régime des Omeyyades, écrasés en 749 à la bataille du Grand Zab. Le nouveau calife, Abu al-Abbas, devient calife en 750. C'est le début du règne de la dynastie des Abbassides.

75 Cette prise de pouvoir traduit une rébellion des peuples contre l'aristocratie arabe. Désormais, aux prérogatives et à la domination d'un classe noble succède la véritable puissance des marchands et commerçants, de la troupe aussi. Ce tournant est civilisationnel aussi. Passage d'un monde à dominante rurale et traditionnelle à un monde où les aspects économiques commencent à peser davantage. Les Fils du Prophète font preuve d'un grand pragmatisme et d'une capacité d'adaptation. Bagdad devient très vite la capitale de ce nouvel Empire musulman. La société et ses arts atteignent à cette période un degré exceptionnel de raffinement mais aussi de cohésion, en particulier sous l'autorité des Calife Harun-al-Rachid et al-Mamun. Règne alors un climat de tolérance, propice à l'échange des idées et des richesses. La structure hiérarchique de la société évolue. C'est la concertation qu'il faut rechercher et qui doit l'emporter, cette concertation qui demeure l'esprit cultivé par les Emirats aujourd'hui encore et dont la structure fédérale actuelle doit rendre compte. Le défi qui s'impose donc dès le VIIe siècle est celui de la conciliation entre une unité pacifiée et la diversité des tribus locales, caressant souvent des aspirations autonomistes. Des siècles plus tard, il semble que le modèle fédéral puisse contribuer à garantir un équilibre harmonieux. En tout cas, il semble relever

l’ancien défi qui se pose depuis de nombreux siècles en l’adaptant au contexte actuel. Aux VIIIe et au IXe siècles, sous la dynastie des Omeyyades puis des Abbassides, par exemple, tandis que la région connaît déjà un réel essor, à bien des titres, dont elle ne profite cependant guère, car il est surtout commercial et sur ses côtes, le bras de fer est constant entre les tribus et les puissances fédératrices. Plus tard, les Perses Bouyides puis les Turcs Seldjoukides tentent d'établir une domination à des fins aussi bien économiques que politiques. Des caravansérails comme Juméirah, l'actuel Dubaï, connaissent une prospérité croissante. Au XIVe siècle, la puissance émergente est le Royaume d'Ormuz qui contrôle de nombreuses îles et des littoraux. L'expansion coloniale marque une rupture autant qu'un nouvel élan. En effet, le Portugal s'implante sur la côte Est du golfe d'Oman et prend Ormuz en 1507. A la même époque, l'Empire ottoman se présente comme son grand rival. Finalement, au bout de plus d'un siècle, les Portugais sont évincés, non sans avoir fortement réprimé les rebelles. C’est alors l’époque de la domination des Qawasim. La tribu arabe qui est alors la plus puissante, dotés d’une flotte équipée et puissante, et comptant sur de solides marins et d’habiles commerçants. Les débouchés sont bien entendu du côté maritime. Mais toute chose a une fin. Les Britanniques, alors puissance maritime montante, soucieuse de dominer une bonne partie du monde écrasent les Qawasim à ras-al-Khaima en 1819, ne laissant derrière eux que ruine et désolation. Mais dans leur esprit pour mieux reconstruire une région pacifiée. Or, donc, en 1820, les Britanniques décident en tout cas de s'entendre avec les cheikhs de chaque émirat pour former ainsi une sorte particulière de confédération. Le renforcement des liens entre chaque émirat tient alors bien entendu à des intérêts commerciaux, mais également à une lutte commune contre les pirates.

76 Malgré l'abolition officielle de l'esclavage, les tensions restent vives et le commerce d'ébène continue. Mais, comme noté plus haut, une certaine stabilité règne depuis la "Trêve perpétuelle" signée en 1853 par les Anglais avec les chefs de tribus. Au demeurant, à cette époque la partie arabe du Golfe reçoit alors pour nom "Côte de la Trêve". Arbitres et pacificateurs, les Britanniques établissent une sorte de paix entre les tribus et les clans qui leur vaut d'apparaître comme la puissance pacificatrice, protectrice de l'ordre et de l'intégrité de chaque peuple de la région. Le rôle et le prestige des Anglais ne cessent de se renforcer avec la menace ottomane. Les Emirats misent de plus en plus sur la protection que va assurer l'armée britannique et qui constitue pour eux une garantie. C'est dans cette optique qu'il faut comprendre la suite des traités entre 1880 et 1892 donnant à l'Empire britannique le contrôle absolu. Les Emirats, en contrepartie sont protégés, en sécurité. Mais, par ailleurs, ils ne peuvent plus prendre d'initiative

diplomatique, ce qui aliène leur indépendance. Nous l'avons déjà dit pour les époques antérieures, et cela vaut pour celle-ci : en fait, les Anglais ne sont cependant guère intéressés par l'intérieur des terres. Quant aux différents émirats ils veulent se garder le plus possible de l'influence ottomane. C'est aussi le cas du Koweït qui n'hésite d'ailleurs pas à faire appel à la flotte anglaise contre l'influence ottomane. Et s'aligne ensuite sur le statut de sujétion qui est celui des autres Emirats. A partir de 1892 d'ailleurs les Emirats finissent par devenir un protectorat relevant de l'empire colonial britannique. Les contours juridiques et territoriaux du protectorat demeurent assez souples. Par exemple, pour éviter tout phénomène de surchauffe, les Anglais se gardaient bien de limiter l'autorité des cheikhs et leur autonomie de décisions. Trois tournants historiques vont cependant contribuer à un réajustement et à des précisions : primo, les conséquences de la Première Guerre mondiale pour l'Empire ottoman, vermoulu, et qui s'effondre; secundo, l'avancée d'Ibn Saoud qui fait figure de conquérant menaçant et tertio enfin, last but not the least, la découverte du pétrole. La dissolution de l'Empire ottoman suite à la victoire de la Triple-Entente (France, Royaume-Uni, Russie) à laquelle s'était jointe l'Amérique sur la Triplice (Allemagne, Autriche-Hongrie, Italie et Empire ottoman) conduit à une reconfiguration importante du monde scellée par le célèbre Traité de Versailles, mais aussi par les Traités moins connus mais également décisifs de Sèvres (1920) et de Lausanne (1923) concernant spécifiquement la Turquie. Si le Président Wilson se pose d'emblée en arbitre afin de modérer les cupidités respectives des uns et des autres et de faire valoir le principe du droit de chaque peuple de disposer de lui-même, il faut hélas reconnaître que les populations locales n'ont jamais été vraiment consultées, de sorte que le nouveau cadastre territorial est source de tensions et de risques de graves conflits.

77 Comme le rappelle justement un spécialiste reconnu de la question, Henry Laurens[46], « en 1914, les provinces arabes de l'Empire ottoman se trouvaient sous l'influence collective et multiforme des puissances européennes, auxquelles s'ajoutaient les Etats-Unis. Les Jeunes-Turcs, au pouvoir depuis 1908, cherchaient à se débarrasser de ces ingérences permanentes, mais au prix d'un centralisme autoritaire qui suscitait l'émergence d'un mouvement autonomiste arabe prêt à chercher des appuis chez les Européens ». Les deux grandes puissances coloniales, pourtant alliées dans le conflit, la France et l'Angleterre, rivalisaient d'influence, désireuses d'étendre leurs conquêtes et leur champ de domination. L'esprit colonial des Britannique put préserver un temps les anciens Emirats de la convoitise ottomane. Quant aux Ottomans, ils veulent

[46] Cf. Henry LAURENS, « Comment l'Empire ottoman fut dépecé » in *Le Monde diplomatique*, avril, 2003, 16-17.

desserrer l'étau colonial, quitte pour cela à brandir la menace d'une guerre sainte. Les Anglais, pour leur part, misent à l'époque sur un soulèvement que peut conduire l'Emir Hussein, de la Mecque. En tout cas, le haut-commissaire en Egypte, Mac-Mahon, correspond avec l'Emir pour l'inciter à se rebeller. Des aventuriers comme Lawrence d'Arabie espèrent eux aussi une renaissance arabe à partir de la dynastie hachémite en bons termes avec l'Angleterre. Les espaces français et anglais sont finalement délimités en fonction des accords secrets conclus en 1916 par les représentants français et anglais François Georges-Picot et Mark Sykes. La question pétrolière commence à devenir primordiale.

78 La défaite de l'Empire ottoman comme en tout cas à la division du Proche-Orient en plusieurs Etats. Ce qui en soi n'est absurde comme le note Henry Laurens. A vrai dire, les Hachémites en avaient déjà caressé l'idée. Les dernières années de l'Empire ottoman avait cependant été marquées par une libéralisation du régime et une ébauche de système démocratique, bien que très imparfait. La façon autoritaire et brutale dont les puissances occidentales entendent régler leur sort ne peut donc être que très mal ressentie par les peuples concernés, qui perçoivent ainsi une régression dans leur destin. Quant aux Emirats, ils ne sont pas directement concernés par le démembrement de l'ancien Empire ottoman n'en faisant pas partie ! Néanmoins l'émergence du Koweït, un temps au statut ambigu, sous la protection de l'Angleterre renforce d'une certaine façon le contrôle britannique sur les Emirats.

79 Il est vrai que ceux-ci redoutent surtout la montée de la dynastie arabique d'Al Saoud. Si l'Arabie saoudite comme telle n'est véritablement créée qu'en 1932, sa constitution progressive s'échelonne depuis le début du XXe siècle, autour de la figure d'Abdelaziz ben Abderrahmane Al Saoud, déjà nommé Wali du Nejd en 1914. Dont il devient roi seulement en 1926. Mais le leader saoudien s'impose d'emblée comme un partenaire incontournable pour les Anglais avec lesquels il signe en 1915 un traité de coopération. L'instauration progressive de la grande Arabie saoudite fait peur aux Emirats. La côte de la trêve semble menacée. Fort heureusement pour les Emirats, un nouveau traité est signé en 1927 entre Abdelaziz et l'Angleterre reconnaissant sa domination sur une large majorité de la péninsule. En revanche, le chef saoudien promet de ne pas menacer l'intégrité territoriale des Emirats. Qui se sentent protégés par le protectorat britannique de leur redoutable voisin.

80 Les bénéfices du commerce des perles se réduisent. Surtout depuis que le gouvernement indien impose des taxes très lourdes à leur importation. A la fin des années 1920, l'activité perlière, un temps florissante, semble désormais entrer en véritable récession. Très vite, elle s'effondre, suite à l'onde choc de la crise économique mondiale. Un autre pays prend le relai de

l'exportation de ce produit toujours fort prisé, le Japon. C'est une leçon pour les Emirats : il est toujours périlleux d'appuyer son développement économique et sa fortune sur un seul produit ou une seule rente. Nous verrons plus loin comme cet avertissement a été pris en compte depuis par des Emirats, en particulier face au spectre de l'après-pétrole, qu'ils anticipent bien plus et bien mieux que d'autres pays pétroliers.

81 Dès les années 1930, dans le cadre de la recherche du pétrole, l'Irak Petroleum Company obtient des concessions à Sharjah et Dubaï en 1937, à Ras al-Khammam en 1938, à Abu Dhabi en 1939 et à Umm al-Qaiwain en 1945. Pour l'instant, il s'agit encore d'un projet et d'une vision prospective. Enfin, entre 1958 et 1960, beaucoup de pétrole est trouvé à Abu Dhabi, en particulier à Murbanqui devient rapidement le gisement le plus important. Un peu plus tard, du pétrole est aussi trouvé à Dubaï et à Charjah. Mais Abu Dhabi doit son essor rapide et ancien à ces découvertes avant que la croissance ne touche les autres émirats. Grâce également au Cheikh Zayed ben Sultan Al-Nahyane qui sait en tirer profit.

82 L'Angleterre allie volontiers au long du XXe siècle une volonté de domination à un réel pragmatisme dans la mise en place d'une organisation destinée à la perpétuer. Londres semble bien surmonter la tentation de la rigidité. Autrement dit, prendre acte, dans une certaine mesure des désirs d'autonomie et les honorer en partie tout en conservant une certaine influence, sous une forme adaptée au nouveau contexte international, désormais marqué par la conviction que chaque peuple doit pouvoir disposer de lui-même. Etranger à une application, abrupte de grands principes, le Royaume-Uni reconnaît par exemple la demande du cheikh de Ras el Khaïmah d'être détaché de Charjah pour former un état autonome. En 1952, il en va de même de Foujeirah²&. A l'évidence, dans l'esprit de l'époque, la bonne harmonie de l'ensemble des Etats n'a rien à perdre d'une marge d'autonomie de chacun d'eux. Ce qui est exactement l'intuition fédérale, même si, alors, cette intuition s'inscrit encore dans le cadre d'un protectorat étranger. La même année 1952, un Conseil des Etats de la Trêve est établi. Prennent part aussi bien les cheikhs que représentants anglais. Les cheikhs, en effet, entendent bien garder leurs prérogatives et exercer leur responsabilité en matière de politique intérieure, au sein de leur Etat. Toutefois, nous ne sommes pas encore dans le cadre d'un Etat fédéral mais plutôt d'une sorte de confédération dans le cadre d'un protectorat comme dit plus haut. Outre les avantages traditionnels liés à la pêche et à la perle, les chefs des Etats bénéficient de plus en plus de rentes, en particulier liées aux hydrocarbures. Malgré la marge de manœuvre et de vraies compensations, la domination anglaise pèse ainsi de plus en plus aux populations autochtones. Par exemple, dès 1953 se met en place à Dubaï un front de rejet de l'emprise britannique.

L'émergence de la Ligue Arabe, en soi assez peu efficace, mais surtout le sentiment d'une identité arabe [47]inquiètent Londres et plus largement l'Occident. Une crise éclate même en 1965, alors qu'un peu partout le colonialisme et même sa perpétuation sous un mode "soft" sont fortement contestés. Le cheikh Saqr Bin Sultan Al Qassimi de Charjah revendique une vraie autonomie, ce qui lui vaut d'être écarté et remplacé par un de ses proches moins intransigeants.

83 C'est la décision du gouvernement travailliste d'Harold Wilson en 1968 d'un retrait rapide de ses forces militaires se trouvant à l'Est de Suez qui ouvre la voie à une évolution longtemps préparée mais qui se réalise plus rapidement que prévue. Les Etats de la Trêve sont traversés par un double sentiment, pratiquement contradictoire. D'une part, ils ne peuvent que se réjouir d'un joug qui s'allège. Mais de l'autre, ils ne se sentent plus protégés, militairement, dans une région pourtant lourde de menaces. Car la présence britannique assure stabilité, sécurité, et une paix même relative. Les Etats de la Trêve se demandent ce qu'il adviendra d'eux, lorsque les garde-fou britanniques ne seront plus là, tandis que deux puissances voisines, plutôt antagonistes, l'Arabie Saoudite et l'Iran tentent d'avoir chacune le plus d'influence possible. L'idée est même avancée de payer à l'Angleterre le coût de son maintien dans la région, ce qui est significatif de l'importance de l'enjeu.

84 Selon le vieil adage, "l'union fait la force". C'est pourquoi, les Britanniques conseillent vivement aux Etats de la Trêve, mais également au Qatar et au Bahreïn, de se fédérer pour pouvoir affronter différents risques. Un accord de principe est même signé entre les neuf souverains. D'autant plus qu'en 1971, la décision britannique de se retirer, est confirmée de façon décevante pour les Etats de la Trêve qui attendaient une politique différente du nouveau gouvernement conservateur d'Edward Heath. Malgré l'urgente nécessité d'un accord à trouver, les chefs arabes n'y parviennent pas. L'une des pommes de discorde est le lieu qui deviendrait la capitale du nouvel état. *Al Khalifa*, soulagé du renoncement de Téhéran à s'emparer de son pays, Bahreïn, en proclame l'indépendance et par là se retire du projet fédéral. Le chef du Qatar fait de même. Les Etats de la Trêve sont ainsi laissés à eux-mêmes.

[47] Cf. Georges CORM, *Pensée et politique dans le monde arabe. Contextes historiques et problématiques XIXe-XXIe siècles*, Paris, éditions la découverte, 2015.

85 Six des sept Etats de la Trêve sont en tout d'accord pour créer un véritable état fédéral : le projet prend corps le 2 décembre 1971. Le septième état qui semblait hésiter, Ras el Khaïmah, ne tarde pas à les rejoindre dès le 10 février 1972. Il semble bien que les réticences de certains cheikhs aient été vaincues par la décision du souverain d'Abu Dhabi de placer une partie de ses revenus, qui tiennent aux réserves en pétrole de l'Emirat, au service de l'ensemble de l'Etat. Au demeurant ce cheikh *Zayed* bin sultan *Al Nahyan* devient alors le Premier Président des Emirats. Un nouvel état fédéral est né.

86 Il est donc certain que l'enjeu pétrolier vint encore renforcer les liens à la fois entre les émirats et avec l'Angleterre[48]. La décolonisation progressive modifie la situation mais sans rupture[49]. Dès le 2 décembre 1971, le lendemain même de la fin du protectorat et donc de la reconnaissance d'un droit à l'indépendance, six des sept émirats se regroupent en un état, rejoints un peu plus de mois plus tard par *Ras al-Khaimah*.

Cette histoire constitue comme le socle sur lequel a pu se bâtir l'organisation et le fonctionnement d'un pays fédéral comme les Emirats. Il nous faut ainsi en cette troisième partie de notre recherche montrer que les Emirats forment bien un état fédéral.

c. Les Emirats. Un état fédéral.

87 D'une certaine façon, les Emirats Arabes Unis forment donc aujourd'hui un hapax au sein du monde arabe, puisqu'ils sont les seuls à avoir adopté pour des raisons à la fois historiques et pragmatiques le modèle fédéral. En réalité, cette singularité tient, comme nous l'avons dit plus haut à l'histoire mais également au fait qu'avant 1971 chacun des émirats disposait déjà de ses propres institutions gouvernementales. Une constitution a été élaborée précisant dans ses articles 120 et 121 quels sont les pouvoirs conférés aux nouvelles institutions fédérales. En l'occurrence, il s'agit de domaines régaliens ou au moins dont le bon fonctionnement suppose une coopération bien harmonisée et articulée, à savoir les affaires étrangères, la sécurité et la défense, la politique des migrations, l'éducation, la santé publique, la monnaie, les postes et

[48] Cf. André BOURGEY, « L'histoire des Emirats arabes du Golfe », in *Hérodote*, Paris, 2009, 133, 92-99.
[49] Frauke HEARD-BEY*, From Trucial States to United Arab Emirates*, Londres, Longmann, 2005.

communications. En revanche, les questions concernant la gestion des ressources énergétiques relèvent de chaque émirat, ce qui est particulièrement à souligner en regard du rôle important que joue le pétrole dans le pays.

88 Chaque système fédéral se compose à sa façon. Dans les EAU, il comprend un conseil suprême, un cabinet ou un conseil des ministres, d'une instance parlementaire, du conseil national fédéral et d'un corps judiciaire. Chacune de ses instances a des compétences qui lui sont propres et leur répartition doit permettre un équilibre. Le plus haut organisme est bien entendu le Conseil Suprême qui élit pour cinq ans le président et le vice-président en charge de la gouvernance au quotidien. Ce conseil suprême élit le conseil des ministres qui suivent chacun les dossiers de leur compétence, mais a charge aussi de ratifier les lois et les décrets fédéraux et de planifier la politique étrangère, sans oublier le rôle parfois plus contester du contrôle des ministres et en particulier du premier d'entre eux. La nature spéciale du fédéralisme des Emirats justifie la pratique selon laquelle le Président est toujours un membre du clan *al-Nahyan* d'Abou Dhabi tandis que le vice-président et premier ministre appartient à la tribu al-Maktoum de Dubaï.

89 Quant au Conseil national fédéral, il se voit soumettre les différentes lois. Lui revient donc l'essentiel du pouvoir législatif. Il se compose de quarante membres dont la moitié est désignée par les responsables de chacun des EAU et l'autre par les instances fédérales, mais de façon indirecte, au travers d'un collège de 6.689 membres au sein duquel sont élus vingt membres du conseil. Il est indispensable que chacun des membres de ce conseil soit effectivement citoyen de l'émirat qu'il est censé représenter. De plus, il doit avoir au moins 35 ans et savoir lire et écrire (au minimum!). Le nombre de membres par émirat représenté tient à la dimension de chacun d'entre eux (de huit pour Abu Dhabi à quatre pour les plus petits émirats). Au sein du Conseil, est élu un Président. Ce conseil remplit aussi un rôle de supervision et de contrôle des décisions prises par les autorités fédérales et les ministres. Il doit aussi donner son avis au sujet des traités et conventions internationales et passe en revue le budget fédéral. Il n'hésite pas à discuter certaines décisions gouvernementales et à se faire écho de plaintes. En tout cas son influence est indéniable dans la rédaction et l'adoption des lois. La majorité des recommandations et des amendements sont en général adoptés.

90 Aux EAU, la législation doit être en harmonie avec la charia. Cela vaut en particulier pour des questions aussi essentielles que sensibles comme le mariage, le divorce et la garde des enfants. Adoptée au début pour une simple durée de 25 ans, la constitution est définitive depuis 1996. Contrairement à un fédéralisme qui naîtrait de l'intention originelle de décentraliser un état d'abord unitaire, les Emirats dérivent d'une volonté de regroupement dans la conviction que l'union fait la force, économique et géopolitique, une force indispensable dans le contexte géopolitique chargé de menaces. On peut donc poser l'hypothèse d'une dynamique de recentrage et d'une tendance à accorder de plus en plus de pouvoir à l'état fédéral. Pour autant, cette orientation dominante n'est aucunement contradictoire avec la volonté farouche de chacun des états fédérés préserver leur gamme d'autonomie et leur liberté d'initiative. Toutefois, il est certain que l'avancée d'un vrai renforcement du modèle fédéral conduit à l'augmentation de la part du budget de chaque émirat destinée à revenir au budget central de l'union. Mais, là encore, comme un mouvement de systole et de diastole, on peut imaginer qu'un renforcement du fédéralisme entraînera non pas en réaction, mais du moins en complément et pour contrebalancer tout risque de déséquilibre du système, un développement des instances propres à chaque émirat fédéré. C'est au demeurant déjà le cas à Abu Dhabi et à Dubaï, les deux entités les plus peuplées et les plus puissantes. En effet, dans le cas d'un état fédéral, il convient sans doute de tenir compte des potentialités propres à chacune des entités qui ne sont en général pas les mêmes de sorte que leur organisation est très diversifiée, par exemple certaines subissent un climat plus ingrat, désertique, et d’autres bénéficient de plus larges débouchés maritimes. Différentes agences d'information, de recherche et de décision existent dans des Emirats par exemple au sujet de la politique de l'environnement, qui devient de plus en plus urgente, ou encore celle du tourisme, du patrimoine naturel et bâti. Ainsi Abu Dhabi ou Sharjah ont-ils leur propre conseil national, organe consultatif. En raison de l'importance numérique de leur population, et de la complexité des responsabilités qui leur incombe, des émirats segmentent leur organisation interne. Par exemple, Abu Dhabi se divise en deux régions, est et ouest. De plus, ses deux villes principales ont chacune leur propre administration municipale.

91 Comme nous l'avons remarqué dans la partie historique de l'introduction, il y a sur la péninsule arabique une tradition de concertation et d'échange entre les dirigeants et leur peuple, de façon régulière, évitant toute accumulation du ressentiment et de la frustration. La tradition arabe est attachée à la participation de tous à la prise de décision et à la recherche du consensus, sous la forme traditionnelle du *majlis*. Ce dernier fait encore partie aujourd'hui du patrimoine

immatériel des Emirats[50]. En principe, la discussion porte sur des questions d'intérêt plus local et davantage circonscrit. L'augmentation de la population a rendu plus délicats des processus démocratiques de ce type qui conviennent à des espaces très limités. Du moins, tant que la numérisation n'est pas encore intervenue car il maximalise la rapidité de la communication et de l'information. La complexité des décisions et leur caractère plus technique rendent cependant de fait improbable, avant peut-être le plein essor encore à venir du numérique, le recours à de telles modalités de concertation. Il devient de toute manière plus difficile de rencontrer le cheikh personnellement. Il n'en demeure pas moins que la tradition des *majlis* perdure bel et bien, et se prolonge dans un idéal de participation qui se trouve au cœur de l'idéal démocratique. Ce dernier n'est pas forcément réductible aux modèles de l'Europe occidentale, comme notre république française. Elle constitue un idéal moral, philosophique, politique et juridique complexe[51]. Les émirats cherchent à conserver et à améliorer un style bien à eux de participations de tous, dans une culture de la concertation que peut sans doute permettre davantage le numérique. Cette forme de participation politique exprime en tout cas une volonté de démocratie directe à laquelle la numérisation pourrait répondre de façon différente. Depuis décembre 2005, le Président Khalifa recommande d'amplifier le rôle du Conseil afin de garantir le respect le plus rigoureux du droit mais également de contrôler la régularité des procédures, ainsi que la transparence ou encore l'égalité des chances. Il est ainsi question d'une modification de la constitution pour accorder une plus large place au Conseil national fédéral. Enfin, depuis 2007, une stratégie gouvernementale est à l'œuvre qui vise à définir une nouvelle administration bien entendu plus efficace - mais quel gouvernement ne poursuit pas ce but? - en particulier dans l'optique d'une synergie mieux articulée et plus cohérente entre les initiatives locales et les décisions fédérales. Il ne s'agit pas seulement de bien répartir, de mieux distribuer les compétences mais d'une part d'éviter des conflits sur certains points et, d'autre part, de susciter une dynamique associant les uns et les autres. Cela implique à l'évidence une modernisation des fonctionnements en vigueur mais également une amélioration qualitative et déontologique

[50] Mario SEBIANE, Patrimoine culturel immatériel dans le golfe arabo-persique. De la construction nationale aux enjeux économiques aux Emirats Arabes Unis (1971-2010), texte disponible sur internet, http://www.wikipci.fr/page/%C3%89mirats_Arabes_Unis)

[51] Cf. Hans KELSEN*, La démocratie, sa nature, sa valeur,* Paris, nouvelle édition, éd. Economica, 1988. En définitive, au-delà de ses formes concrètes de réalisation, la démocratie serait une sorte d'équilibre à trouver entre la protection de la liberté de chacun et le maximum d'égalité. Ce que l'on présente de façon classique comme une démocratie pourrait bien ne pas l'être, car en réalité ne faisant appel que de façon assez formelle et parfois même diversement manipulée au peuple au moment des élections, ce que déplorait déjà, nous l'avons dit, en son temps, Jean-Jacques Rousseau. Et, à l'inverse des formes nouvelles de démocratie pourraient également apparaître, en résonance avec l'histoire propre d'un pays, comme le suggère l'essai percutant et dérangeant, Luciano CANFORA, *La démocratie. Histoire d'une idéologie,* tr.fr. de Anna COLAO et Paule ITOLI, préface de Jacques LE GOFF, Paris, Seuil, col. 'Sciences Humaines', 2006.

dans le sens de la démocratisation. Or, la révolution numérique ne s'inscrit pas simplement dans un héritage ou dans un modèle, dans des limites qui précède sa venue. D'une certaine façon, comme dans toute rencontre, il y a une sorte d'interférence réciproque et de modification de l'un par l'autre. Cela est d'autant plus vrai dans le cadre de la révolution numérique qu'elle semble comme créer sa propre géographie, sa propre cartographie, et ainsi redessiner les frontières, déplacer des limites, en annuler et en introduire de nouvelles.

92 Cela fait des années que la géographie s'intéresse au cyberespace[52]. Emerge ainsi une tout autre approche de l'espace que celle du relief ou du développement industriel. En tout état de cause, le cyberespace nous laisse voir un tout nouveau champ d'investigation, avec des défis plus complexes, des enjeux davantage articulés, des rapports de force qui ne sont pas toujours faciles à identifier, mais également des reconfigurations parfois mouvantes ou indécises, et quelquefois radicales. On peut parler d'un nouveau type de géographie humaine impliquant à la fois une nouvelle cartographie[53] mais également une vraie géopolitique[54]. A l'évidence, cette évolution conteste et déplace frontières et limites.

[52] Martin DODGE et Rob KITCHIN*, Atlas of Cyberspace*, Londres, Pearson, 2001 ; Stephen GRAHAM et Simon MARVIN, « Planning cybercities : Integrating telecommunications into urban planning » in *Town Planning Review*, 70, 1999, 89-114 ; Barney WARF*, Global geographies of the Internet*, Londres, Springer, 2013.

[53] Frédérick DOUZET (dir.), « Cartographie du cyberespace » in *Etude prospective et stratégique*, Paris Ministère de la Défense, 2016 ; Aharon KELLERMAN, *Geographic Interpretations of the Internet*, Londres, Springer, 2016.

[54] Frédérick DOUZET, « La géopolitique pour comprendre le cyberespace » , *Hérodote*, 2014, 152-153, 3-21.

Section II. La mise en cause, à l'ère du numérique, des limites institutionnelles

a. Les frontières mises en question.

93. En raison de leur histoire que nous avons largement évoquée précédemment, les Emirats entretiennent bien entendu avec la notion de frontière un rapport très différent de celui de la France. Le sentiment de constituer une nation n'est à l'évidence pas du tout identique dans le cas d'un pays unitaire qui s'est formé il y a très longtemps, a connu un idéal de centralisation comme le jacobinisme [55] et, le connaît encore aujourd'hui dans une certaine mesure, et dans le cas d'une agglomération de type fédéral d'entités constituées à partir d'une histoire ancienne et tribale. On peut voir dans le cas particulier des Emirats un vestige d'une situation moins élaborée et plus archaïque ou au contraire un contexte favorable, justement, à une façon plus souple et différenciée de tracer des frontières, moins rigide, parfois moins linéaire, mais dans une perspective plus pragmatique. Comme le relève William Guéraiche dans une étude fouillée sur les Emirats : "le territoire était pensé comme le support de l'économie traditionnelle permettant l'exploitation de ressources naturelles sans que n'interfèrent les notions de propriété ou d'exploitation exclusive"[56]. Les partages territoriaux sont également associés, de façon traditionnelle, à l'autorité d'un chef de tribu ou d'un responsable religieux[57]. La notion de territoire est ainsi subordonnée à celle d'influence autorisée et déclinée sans être absolutisée, comme une réalité aussi bien intangible qu'arbitraire. Au demeurant, les marges des territoires sont assez larges et incertaines. Le plus important est la cohérence d'une unité dans l'espace garantie par une autorité, des valeurs et quelquefois une activité économique ou commerciale commune. Il en allait de même en Occident, au moins dans une certaine mesure, au Moyen Age et à la Renaissance. Il serait simpliste de n'y voir qu'un reste du passé. Au contraire, ces volontés de tracer des frontières qui aient du sens, de différentes manières possibles, une cohérence économique ou historique, au lieu de tracer des lignes de manière arbitraire par obligation de diviser des espaces - ce qui risque toujours de multiplier les risques de conflits et même de guerres, en particulier dans un monde où les frontières se multiplient comme le nôtre [58]-

[55] Pierre ROSANVALLON, *Le modèle politique français, la société civile contre le jacobinisme de 1789 à nos jours,* Paris, Seuil, L'Univers historique, 2004.
[56] William GUERAICHE, *Géopolitique de Dubai et des Emirats arabes unis*, Nancy, Arbre bleu éditions, 2014, 57.
[57] Cf. l'étude décisive : John C. WILKINSON, "Traditional concepts of Territory in South East Arabia", in *Geographical Journal*, 149, 3, 301-315, 1983.
[58] Michel FOUCHER*, L'obsession des frontières*, Paris, Librairie Académique Perrin, 2007.

pourrait bien s'harmoniser avec la remise en cause des frontières traditionnelles introduite par le numérique, et une notion différente de la souveraineté[59].

94. Paradoxalement, les Emirats cultivent sans doute une conception assez souple de la frontière lors même que, pour eux, certaines délimitations et répartitions territoriales se présentent comme d'une importance vitale. Les litiges frontaliers avec d'une part et surtout Oman, mais aussi l'Arabie saoudite, ont longtemps perduré et d'une certaine façon demeurent au moins comme une menace qui plane[60]. Pour l'essentiel, un compromis a été trouvé avec l'Arabie saoudite scellé par le traité de Djeddah de 1974, mais c'est plus tardivement, en 2008, que les 272 kilomètres de frontière avec Oman ont été définis. Les Emirats sont nés sur des compromis entre prétentions territoriales par exemple entre Abou Dhabi et Dubaï. Cet art du compromis n'est pas inutile pour préciser le sort d'îles sous influences rivales. Un exemple souvent mentionné est celui de *Buraimi,* une ville oasis du sultanat d'Oman, qui forme un Gouvernorat à la frontière avec les Emirats, et en particulier avec la ville d'Al Ain. Cette proximité géographique pourrait certes devenir explosive mais illustre aussi une capacité à une vraie cohabitation territoriale dominée par le pragmatisme, bien significative d'une certaine vertu traditionnelle de cet espace géographique.

95. Il est certain que la révolution numérique se caractérise d'emblée par une maximalisation de la rapidité des opérations et des démarches, par des facilités accrues. Mais cette évolution n'est pas seulement à définir en termes d'efficacité. Elle induit d'ores et déjà, indépendamment de toute mise en perspective par le droit, un déplacement, choisi ou non, mais s'imposant comme un corollaire, dans la représentation du monde, dans son découpage géographique et institutionnelle, alors que les anciennes frontières demeurent sur le papier ou dans les traités. Appréciée ou maudite, cette révolution numérique encore en cours est aussi d'une certaine façon déjà accomplie. Or, pas plus qu'un virus ne s'arrête à une frontière - hélas pour la santé publique et comme le confirme la récente pandémie du Covid19 - les effets d'internet ne se laissent circonscrire par des mesures protectionnistes, déjà parce qu'ils les précèdent

[59] J. E. PETERSON, "Sovereignity and boundaries in the Gulf States. Setting the Peripheries" in Mehran KAMRAVA (dir.), *The International Politics of the Persian Gulf*, Syracuse, Syracuse University Press, 2011, 21-49

[60] Cf. Aqil KAZIM, *The United Arab Emirates AD 600 to the Present. A socio-discursive Transformation in the Arabian Gulf, Dubaï*, Gulf Book Centre, 2000, 217-233; Fatma AL SAYEGH, "The UAE and Oman : opportunities and challenges in the twenty-first century" in *Middle East Policy,* 9, 3, 124-136, 2002.

chronologiquement. Le législateur est ainsi obligé de faire preuve d'une grande humilité. En effet, il doit affronter un phénomène sociétal à l'échelle planétaire, même si c'est avec une importance différente, qui le précède et souvent le contrarie en amont. A l'évidence, l'un des effets les plus manifestes, étonnement rapide, de la révolution numérique réside dans un bouleversement du cadastre mental et institutionnel du monde, en contraste avec les découpages officiels et juridiques. Toutefois il ne s'agit pas, nous semble-t-il, d'une revendication initiale, de type idéologique, dont le numérique serait le moyen de réalisation mais plutôt d'un phénomène qui, selon l'expression fort juste du sociologue Edgar Morin, participe de l'émergence[61]. L'émergence ne traduit pas un programme, un plan concerté, mais advient en quelque sorte en bonne part par surprise, sauf à élaborer une très hypothétique théorie du complot, ou une providence divine. En d'autres termes, une mutation importance de la société est aujourd'hui largement engagée, induite par de fabuleuses potentialités technologiques, mais sans avoir été préparée au préalable par une spéculation philosophique ou une recherche utopique, de sorte qu'elle nous prend largement de court, et force le juriste et les divers pouvoirs législatifs à réfléchir en quelque sorte dans l'urgence et en aval.

96. La révolution numérique est un phénomène global aux contours diversifiés concernant aussi bien la sphère privée que publique. Comme la révolution industrielle du XIXe siècle, elle se présente avant tout comme la conséquence d'un changement technique, en l'espèce, comme chacun sait, la numérisation de l'information[62]. Trois tournants notables ponctuent l'avancée de la révolution numérique : D'abord, l'apparition de l'ordinateur personnel et de la possibilité de voyager sur la toile dans le cadre individuel; ensuite, sous la forme de la constitution de réseaux; enfin, avec la diffusion du smartphone. Par-là, les barrières anciennes, qui furent longtemps physiques, imposant des exigences difficiles, telles traverser des montagnes comme les éléphants d'Hannibal, ou les mers, tombent largement, et d'une certaine façon toutes seules, dans l'obsolescence. Non seulement les informations circulent sans être retenues mais la mentalité même des individus s'en trouve fortement modifiée. Il est vrai que cette révolution a été précédée par d'autres que d'une certaine façon elle ne fait que poursuivre comme le chemin de fer, l'électricité, l'avion ou le téléphone. C'est pourquoi, d'ailleurs, du point de vue qui est le sien de l'histoire sur une longue durée, Luc Ferry estime-t-il justement que la révolution

[61] Cf. Alfredo PENA-VEGA, "L'émergence d'un nouveau mode de pensée" *in Hermès / La Revue*, 2011/2, 60, 86-92)

[62] Cf. pour une présentation de base mais consistante : Milad DOUEIHI, *Qu'est-ce que le numérique ?* Paris, Presses Universitaires de France, 2013.

numérique s'inscrit justement dans une suite de mutations, mettant en cause un ordre ancien, pour en faire émerger un nouveau, mais dans une suite qui est celle de l'ensemble de la révolution industrielle[63]. La révolution numérique se présente toutefois bien avec une spécificité qui est l'interconnexion rapide. Au temps du progrès du chemin de fer, par exemple, par imitation ou émulation, un autre pays pouvait lui aussi poser des rails. Le propre de la révolution numérique tient au fait que ce qui se passe quelque part touche tout le reste de la planète, par le fait même. Elle forme d'ailleurs un ensemble, la moindre évolution de l'un de ses éléments conduisant à une recombinaison de l'ensemble. Le philosophe Jacques Ellul, prompt à critiquer les conséquences du progrès technologique définit le système comme "un ensemble d'éléments en relation les uns avec les autres de telle façon que toute évolution de l'un provoque une évolution de l'ensemble, toute modification de l'ensemble se répercutant sur chaque élément"[64]. A cet égard, nous assistons peut-être à un tournant qui n'a jamais eu son pareil.

97. Dès les années soixante, Marshall McLuhan (1911-1980), sociologue et théoricien canadien de la communication, a posé la notion de "village planétaire" [65] pour montrer l'effondrement des frontières et des barrières au profit d'un message dont le mode de communication revêt souvent plus d'importance que son contenu même, contenu en partie forgé par la transmission elle-même qui ne se contente donc pas de se placer à son service, selon l'ancienne conception, mais façonne aussi le message comme l'étudie la médiologie[66]. Cette communauté de médium l'emporte sur la diversité des contenus de sorte que l'humanité s'achemine vers la formation d'une seule tribu numérique. La mise en cause des formes traditionnelles de l'écrit conduit à une nouvelle universalité, dont on peut cependant douter de la qualité. Dans la diversité, une communauté se forme, transversale et transfrontière, dont on a du mal à comprendre comment elle pourrait bien s'accommoder des délimitations traditionnelles. Avec le nouveau millénaire et le passage d'internet en haut niveau au début des années 2000, le numérique s'installe dans les foyers. La dématérialisation des moyens d'information et des activités humaines rend dérisoires les anciens barrages. Pourtant, il faut savoir que la consommation des centres de données dépasse celle du trafic aérien et qu'une simple recherche sur Google produit aussi du CO2, de sorte que le virtuel

[63] Luc FERRY*, L'innovation destructrice*, Paris, Plon, 2014.
[64] Jacques ELLUL*, Le système technicien*, Paris, 3 éd., Cherche Midi, 2012, 14.
[65] Marshall McLUHAN, *La galaxie Gutenberg : la genèse de l'homme typographique*, Montréal, HMH, 1964; Marshall McLUHAN*, Pour comprendre les médias*, Paris, Seuil, Points, 1968; Marshall McLUHAN, *Guerre et paix dans le village planétaire,* Paris, Robert Laffont, 1970.
[66] Régis DEBRAY, *Introduction à la médiologie,* Paris, PUF, 2000.

n'est aucunement l'immatériel ou le purement spirituel. Toutefois des notions comme celle de propriété intellectuelle deviennent difficiles à circonscrire et impossibles à protéger. Une nouvelle criminalité peut se développer, mais le combat contre la criminalité dispose lui aussi de toutes nouvelles armes, par-delà les frontières. Des écrivains et des journalistes, comme Marc Dugain ou Christophe Labbé par exemple estiment que la révolution numérique "ne se contente pas de modeler notre mode de vie vers plus d'information, plus de vitesse de connexion, elle nous dirige vers un état de docilité, de servitude volontaire, de transparence, dont le résultat final est la disparition de la vie privée et un renoncement irréversible à notre liberté"[67]. Ce danger ne saurait être minimisé par le juriste. Nous y revenons par la suite. Aucune frontière classique tracée par l'homme ne peut empêcher cette évolution. Certes, les inégalités économiques et de développement technologique maintiennent encore ce que l'on appelle la fracture numérique, à savoir une disparité géographique d'accès, localisable sur une carte, entre pays plus développés et pays moins développés, mais également entre centres urbains et périphérie campagnarde. Du point de vue plus étroitement juridique, cela peut poser la question d'un éventuel droit à une connexion numérique. Si l'importance de cette fracture devait être confirmée, comme le suggère en France le Rapport de Jacques Attali de 2016, cela voudrait dire que les nouvelles technologies n'effacent pas seulement les frontières mais d'une certaine façon en créent de nouvelles, en fonction de la richesse par exemple, ou si l'on préfère les déplacent. Mais l'on peut aussi émettre l'hypothèse selon laquelle cette fracture ne serait en fait qu'un état intermédiaire entre l'absence de développement du numérique et sa diffusion générale, à savoir au cours d'une période dans laquelle le numérique s'implante partout mais progressivement, selon une vitesse qui n'est pas égale. La fracture numérique, toutefois, ne concerne pas seulement l'accès ou non à internet, mais les lieux d'hébergement de sites, auxquels il faudrait se connecter. Enfin, il semble que nous nous trouvons actuellement dans une phase de transition, la révolution numérique étant déjà largement engagée, toutes ses ressources étant identifiées et de plus en plus disponibles, lors même que toutes ses incidences n'apparaissent encore pas clairement. Une crise comme celle du Covid-19 il y a peu, avec un temps de confinement très long, peut d'une part manifester cruellement cette inégalité induite par un accès à internet qui n'est pas partagé par tous mais aussi favoriser un peu par la force la familiarisation des plus rétifs ou des moins à l'endroit de nouveaux moyens qui deviennent de plus en plus incontrôlables.

[67] Marc DUGAIN et Christophe LABBE*, L'homme nu, la dictature invisible du numérique*, Paris, Robert Laffont/Plon, 2016, 7.

98. Manuel Castells a cependant mis en évidence la spécificité d'une société en réseaux comme celle propre à l'ère de l'information qui est la nôtre[68]. Un réseau est un ensemble d'éléments, d'individus, d'organisations et de villes qui forment une unité mais sans faire perdre leur individualité aux personnes ou aux groupes, au travers des échanges et interactions. On songe bien entendu d'emblée à ce que la société en réseaux présente en commun par rapport au régime fédéral qui en est comme l'anticipation ou l'analogue institutionnels. Bien entendu, un réseau peut-être structuré hiérarchiquement, sans aucune incompatibilité absolue. Néanmoins on peut dire que, de soi, un réseau se présente moins facilement comme hiérarchisé car c'est l'articulation de tous les éléments qui le conglomèrent, beaucoup plus qu'une autorité intérieure ou extérieure, qui le constitue. L'une des caractéristiques du réseau pour Castells semble être précisément sa faculté d'évolution en fonction aussi bien de la dynamique qui la traverse et l'anime que du contexte qu'il doit affronter et des variations des éléments, ce qui en fait une configuration mouvante plutôt que pétrifiée. Le réseau ne se réduit pas seulement à une organisation de l'information qui se diffuse et se communique mais forme une sorte d'espace citoyen à l'échelle du monde, et sans frontières traditionnelles. Le caractère incontrôlable du net contribue à l'implantation d'une mentalité libertaire. Dans un livre récent [69]Castells établit d'ailleurs que le succès du numérique, tient consciemment ou inconsciemment à sa capacité à contourner les cadres institutionnels et bureaucratiques traditionnels, plus limitatifs pour l'épanouissement individuel. Le réseau est profondément décentralisé, ce qui favorise les échanges.

99. Au-delà des effets immédiats induits par les technologies elles-mêmes, qui semblent se moquer des frontières traditionnelles et des découpages institutionnels, il semble que le numérique nous pousse aussi à la remise en cause intellectuelle d'anciennes valeurs légitimant bien des limites et des frontières. Ainsi, ces dernières peuvent-elles légitimement paraître datées, obsolètes, inutiles voire nuisibles par exemple face à de nouveaux défis à relever. Cela vaut ainsi de la lutte contre la criminalité, en particulier de la lutte contre la cybercriminalité, et a fortiori contre le terrorisme, mais aussi contre les contrefaçons[70]. La porosité des anciennes frontières place

[68] Manuel CASTELLS, *L'ère de l'information, I, La société en réseaux*, Paris, Fayard, 1998 ; II, *Le pouvoir de l'identité*, Paris, Fayard, 1999 ; III, *Fin de millénaire,* Paris, Fayard, 1999)
[69] Manuel CASTELLS, *La galaxie internet*, Paris, Fayard, 2001.
[70] Franck GUARNIERI, "cybercriminalité et contrefaçons : pour une nouvelle analyse des risques et des frontières" *in Hermès / La Revue*, 2012 / 2, 63, 75-80.

nos sociétés dans une situation obsidionale qui les contraignent soit à renoncer à se défendre et à repousser des assaillants indésirables, soit, en revanche, à trouver et surtout à mettre en place de nouvelles stratégies de défense, adaptées et efficaces[71]. Une zone frontière, évidemment analytique, entre tout l'espace du réel et tout l'espace du virtuel peut être envisagée non seulement comme tampon mais comme échange même si le réel et le numérique ne deviennent pas hybrides pour autant et gardent leurs spécificités y compris dans les frontières qu'elles s'imposent ou qu'elles tolèrent, dans le cadre d'une globalisation complexe et polymorphe[72]. Mais Guarnieri a surtout raison de montre combien le numérique introduit des "déstabilisations hiérarchiques" (op.cit.) dont il faut prendre la mesure. Autrement dit, les frontières et surtout leur justification ne peuvent demeurent les mêmes sans un processus de révision. On observe plutôt un entrecroisement de différentes frontières qu'il s'agit d'harmoniser.

100. Or, le numérique n'est pas né au sein de structures institutionnelles et n'en respecte pas les configurations spécifiques. Ce constat premier explique pourquoi il ne recouvre pas les divisions et les organisations mais établit son ordre à lui, bien différent. Au point de vue juridique, cela pose d'emblée un certain nombre de problèmes concrets. Le respect de la vie privée par tel site internet situé dans tel pays ne vérifie pas les exigences qui s'imposeraient dans un autre pays. Or, ce site est visité par des personnes du monde entier, vivant chacune dans un pays, avec une régulation précise sur la question mais qui n'est pas la même. En matière de droit pénal, ce qui sera accepté ici, ne le sera pas ailleurs. Un exemple délicat permet de mieux comprendre, celui de la prostitution et du racolage, tout simplement parce que la législation sur ces questions varie beaucoup d'un pays à l'autre. Différents sites internet peuvent proposer de "l'accompagnement", ou de la location d'"escortes" dans les faits, souvent des prostituées déguisées. Or, en France, le racolage sexuel en vue d'une relation rémunérée est en théorie lourdement condamné et considéré depuis la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure comme un délit, surtout lorsqu'on favorise ainsi la prostitution d'un autre même sans but lucratif personnel. Ainsi l'article 225-10-1 du code pénal peut-il énoncer : " le fait, par tout moyen, y compris par une attitude même passive, de procéder publiquement au racolage d'autrui en vue de l'inciter à des relations sexuelles en échange d'une rémunération ou d'une promesse de rémunération est puni de deux mois d'emprisonnement et de 3750 € d'amende». Mais internet permet de contourner cette répression. Il suffit que le site ne soit pas hébergé en France, mais

[71] Zygmunt BAUMAN, *La société assiégée*, Paris, Hachette Littératures, 2007.
[72] Cf. Saskia SASSEN*, La globalisation*, Paris, Gallimard, 2009.

par exemple en Allemagne, où la prostitution et le racolage sont autrement considérés du point de vue légal. Pourtant s'inscriront sur ce site des personnes vivant en France par exemple, et racolant donc sur ce territoire. Internet permet ainsi un contournement, peu discret en outre dans ce cas précis, de la loi.

101. Un autre exemple peut encore être donné, celui des téléchargements et des contrefaçons[73]. Les Emirats présentent évidemment une situation plutôt favorisée en matière d'accès à internet. Les grandes villes bénéficient toutes de la fibre optique. Toutefois, un certain contrôle d'internet et une certaine censure existent déjà. Les risques de cyberterrorisme sont vivement combattus et il n'est pas possible d'avoir accès à des sites présentant des risques de violence terroriste. Il en va de même des sites de rencontres érotiques, ou de sites à connotation indécente par exemple avec des images de nudité. Les Emirats entendent censurer la pornographie*, le hacking* mais aussi les jeux d'achat en ligne, mais aussi la critique des religions et en particulier de l'islam. Bien entendu, une censure s'exerce également en ce qui concerne la critique du gouvernement et de la famille régnante. Le contrôle est fait de façon très rigoureuse et très efficace. Les sites censurés sont signalés par un petit écran gris, accompagné d'un lien, de sorte que l'internaute est renseigné clairement des raisons de la censure et plus largement de la politique en vigueur Les raisons invoquées pour pratiquer une telle censure sont des raisons de sécurité nationale ou d'éthique, comme la France censurent pour sa part aussi certains sites, pour lutter contre la pédopornographie et le négationnisme par exemple mais en nombre moins nombreux. Skype même est censuré mais non pas son utilisation pour communiquer. Ces règles rigoureuses n'empêchent pas es citoyens des Emirats et les résidents à pratiquer largement le téléchargement illégal, bien davantage qu'en France selon les études statistiques. En effet, si les sanctions sont très lourdes, il y a toujours beaucoup de chance de passer entre les mails du filet.

102. La répression contre de telles pratiques se met en place aux Emirats. En 2016, le Président des Emirats Arabes Unis, Sheikh Khalifa Bin Zayed Al Nahyan, fit passer une loi assez répressive au sujet des fraudes sur internet, notamment le téléchargement illégal. L'article 1 destiné à

[73] Sur le problème d'ensemble : Victor DZOMO-SILINOU, « Le phénomène du téléchargement illégal sur internet et la question de la rémunération de la création » in *Les cahiers de la propriété intellectuelle*, 2011, 23-2, 7-73 ; du même auteur : « Les législations de la lutte contre le téléchargement illégal : entre riposte graduée et filtrage de l'internet », *in Les cahiers de propriété intellectuelle*, 2014, 26, 1, 43-48.

remplacer l'article 9 de la Federal Law No. 9/2012, stipulait en effet que « quiconque fait usage d'une adresse de protocole de réseau informatique frauduleuse (adresse IP) en se servant d'une fausse adresse ou de l'adresse d'une tierce partie par tout autre moyen dans le but de commettre un crime ou d'en empêcher la découverte, sera puni d'un emprisonnement temporaire et d'une amende n'allant pas en dessous des 500 000 dirhams et ne dépassant pas 2 000 000 dirhams, ou sera puni de l'une de ces deux peines ». Lorsqu'on convertit ces sommes en euros, cela inscrit la peine dans une fourchette 125 000 euros et 500 000 euros. La plus extrême sévérité est donc de mise ce qui ne veut pas dire qu'elle s'avère pour autant efficace. Mais il ne s'agit pas seulement, pour les Emirats, de combattre le téléchargement illégal mais encore de bloquer les fonctionnalités d'appels aussi bien vidéo qu'audio sur des applications de messageries populaires comme Snapchat 2.0. Il faut savoir en effet que sa mise à jour permettait aux utilisateurs d'activer des chats vidéo ou audio qui se trouvent en violation de la régulation des Émirats Arabes Unis sur les communications *VoIP* qui interdisent aux fournisseurs tiers de proposer des services de téléphonie basés sur internet, que ce soit pour des appels vidéo ou audio. Pourtant, malgré le fait que le *TRA* a clairement fait savoir que l'accès aux services *VoIP* autres que ceux qui sont proposés par des entreprises disposant d'une licence est illégal, certaines personnes continuent bien entendu d'utiliser de tels services par des voies détournées, notamment les *VPN*. Ont quand même continué à utiliser ses services grâce à des *VPN*, les réseaux privés virtuels. Du reste, en soi, ces réseaux ne sont pas illégaux mais les utiliser afin d'avoir accès à des services ou à des contenus bloqués l'est en revanche. En outre, l'association de défense des droits privés *Privat Internet Access* fait remarquer qu'auparavant, la compréhension du droit de l'internet des Émirats Arabes Unis stipulait que l'utilisation d'un *VPN* ou d'un proxy entraînerait des poursuites en vertu de la loi sur les télécommunications uniquement si elle était utilisée dans le contexte d'un autre crime. Il semble que désormais la police des Émirats Arabes Unis soit autorisée à se tourner vers des utilisateurs de *VPN* quel que soit le motif du crime. À l'heure actuelle, de tels crimes incluent l'accès aux services ou sites web bloqués auxquels il n'est pas possible d'accéder sinon avec un *VPN* ou un proxy, utilisation que les Émirats Arabes Unis considèrent dorénavant comme une utilisation frauduleuse d'adresse IP. En clair, cela implique que « téléphoner à son domicile avec des services ne disposant pas de licences (un souci pour la plupart des résidents des Émirats Arabes Unis) tels que *WhatsApp*, *Face-Time* ou Snapchat » n'est pas légal. Qui plus est, les *VPN* sont(bel et bien utilisés par plusieurs personnes sur le territoire pour avoir accès à des versions internationales de certains sites qu'ils visitent comme faire croire à la version américaine de Netflix que l'utilisateur y est résident pour pouvoir avoir accès au service. Les Emirats prévoient en tout

cas des sanctions exemplaires de la piraterie en ligne qui s'applique également aux résidents dans ce pays. Ainsi, en 2016, l'un d'entre eux a-t-il été emprisonné à Abu Dhabi pour avoir volé et illégalement uploadé une suite de séries télévisées et de films de la plateforme de télévision OSN. Il a été condamné à six mois de prison et à verser 50 000 dirhams (12 500 euros) à OSN en guise de dommages et intérêts. Il sera expulsé vers son pays d'origine une fois sa peine purgée[74].

103. La propriété intellectuelle est fortement protégée dans les Emirats dans un cadre jurdique très défini et minutieusement révisé en 2002 dans un sens conforme aux règles internationales car les Emirats y ont notamment ratifié les conventions internationales suivantes gérées par l'OMPI (Organisation Mondiale de la Propriété Intellectuelle) : Conventions de Paris, de Berne, de Rome, Traités de l'OMPI sur le Droit d'Auteur, et sur les interprétations et exécutions et les phonogrammes. En matière de brevet d'inventions, les Emirats ont rejoint le Patent *Cooperation Treaty* (PCT); membres du Conseil de Coopération des Etats Arabes du Golfe (CCEAG), ils ont intégré le système de brevet unifié de cette organisation. Membres de l'OMC depuis 1996, les Emirats sont signataires de l'accord ADPIC (Accord sur les Aspects des Droits de Propriété Intellectuelle qui touchent au commerce). La sévérité implacable avec laquelle Emirats entend lutter contre la contrefaçon n'empêchent pas celle-ci de proliférer aussi sur le territoire émirien lui-même que sur les navires du port de Dubaï. L'office de propriété intellectuelle des Emirats dépend du ministère de l'économie et les services de dépôt de titre sont regroupés au sein d'un département spécifique voué à la protection de la propriété intellectuelle. On y distingue le bureau des marques et celui des brevets, mais également celui du droit d'auteur et du droit voisin. Tout est très bien organisé et mis en place. Il est intéressant de signaler un premier accord de coopération sur la propriété intellectuelle entre la France et les Emirats signé en 2008. Dix ans plus tard, un autre accord a été signé en 2018, entre le centre national d'enregistrement des brevets émirien et l'institut national de la propriété industrielle français. Les Emirats connaissent plusieurs types de propriété intellectuelle[75]. D'abord le brevet d'invention qui protège une innovation technique qui apporte une véritable nouveauté absolue d'un point de vue technique, bien entendu hors exclusion à la brevetabilité et inventions contraires à l'ordre public et aux bonnes mœurs (ce qui pourrait par exemple être le cas des

[74] https://www.developpez.com/actu/101890/Ne-vous-risquez-pas-a-utiliser-un-VPN-aux-Emirats-Arabes-Unis-sauf-si-vous-etes-pret-a-payer-une-amende-de-500-000-et-faire-de-la-prison/
[75] *https://www.tresor.economie.gouv.fr/Pays/AE/propriete-intellectuelle*

inventions liées à la fabrication d'alcool). La marque, quant à elle, doit être distinctive, disponible et licite mais il faut en outre qu'elle ne contredise pas les valeurs essentiels de l'Islam (rejet des marques pour les boissons alcooliques, les casinos, les discothèques, les produits à base de porc). La procédure d'opposition est ouverte pendant 30 jours après la publication de la marque. Les dépôts multi-classes ne sont pas possibles aux Emirats : un dépôt par classe est nécessaire. Enfin, dernier type, le dessin et le modèle doivent avoir une apparence spécifique, se présenter comme nouveau et être utilisé dans l'industrie ou l'artisanat.

104. Le téléchargement sans respect du droit d'auteur est illégal en France et copier sur son ordinateur un film ou une musique, peu importe par quel procédé, peut alors relever du délit. Bien entendu, les facilités du numérique font qu'un tel délit est souvent commis et par conséquent très rarement réprimé, de sorte que la plupart du temps, mais pas toujours, le délinquant est de fait de l'assuré d'une certaine impunité, ce qui n'est d'ailleurs pas seulement vrai pour des délits liés au numérique mais par exemple pour la consommation personnelle de certains stupéfiants. Mais si le téléchargement a eu lieu ailleurs, par exemple sur un ordinateur étranger, et est placé sur une clé ou un disque amovible, le cas est plus complexe, même si le téléchargement d'une copie illégale est de toute façon frauduleux. En théorie la contrefaçon est fortement réprimée en France, comme l'atteste l'article L335-2 du code de la propriété intellectuelle. Elle est punie de trois ans d'emprisonnement et de 300.000 euros d'amende. Quand le délit a été commis en bande organisée, les peines sont portées à sept ans d'emprisonnement et à 750.000 euros d'amende. Poursuivre judiciairement des millions de Français n'aurait guère de sens. Le problème n'est pas tant de trouver des solutions juridiques cohérentes et claires aux cas de figures qui peuvent se poser, et qui se posent un très grand nombre de fois, mais de façon beaucoup plus simple et plus radicale celui du caractère décalé d'une volonté d'appliquer des règles variables selon les états et qui ne semblent plus du tout adaptées aux pratiques actuelles. Dans le train qui longe la côté de Montpellier à Barcelone, c'est seulement après avoir franchi la frontière espagnole que se met en marche un système de télévision permettant de voir un film, en raison de la différence de législation. D'une certaine manière, il devient de plus en plus inacceptable de tracer ainsi une ligne de partage entre deux pays pour des biens presque par essence aussi volatiles que les prouesses numériques. Le fait accéléré de la circulation des personnes, au-delà des problèmes casuistiques posés, comme celui de la nationalité d'un bébé qui naîtrait dans un avion, laisse voir de façon cruelle combien un certain ordonnancement de l'espace du monde associé à des législations insuffisamment

harmonisées est en décalage avec un phénomène émergent, incontournable et sans doute incontrôlable de bien des points de vue. En règle générale, la législation est avant tout territoriale de sorte que la personne est tenue de respecter les lois du pays où elle se trouve même si ce n'est pas le sien, l'inverse n'étant pas vrai, sauf pour des crimes très graves, comme les crimes contre l'humanité, ou le tourisme sexuel (afin de réprimer le tourisme sexuel au détriment de mineurs, un ressortissant français peut être poursuivi même si son crime a eu lieu hors du territoire français et n'est pas poursuivi dans le pays concerné : art. 222-24 (2) du code pénal). Mais ce principe d'imputabilité semble étrangement impropre depuis que la révolution numérique inscrit des délinquants d'un nouveau genre dans un espace transfrontière d'internet qui n'est pas plus celui des législations nationales.

b. *Révolution numérique et modèle fédéral*

105. Il est moins évident en revanche de discerner un lien entre le numérique et la valorisation ou la contestation d'un modèle politique de type fédéral. La numérisation semble induire un mouvement paradoxal. En effet, d'une part, il favorise la concentration et l'influence du pouvoir central, qui a longtemps été miné dans ses ambitions centralisatrices par les distances à franchir. On peut même aller jusqu'à penser que, d'une certaine manière, l'idéal de l'état centralisé demeure plus ou un vœu pieux ou à la portée limite si l'infrastructure technologique ne permet pas une mise en œuvre concrète, par exemple en raison d'espaces géographiques gigantesques comme ce fut le cas après la révolution en Russie, avec en *contrepartie* de cette difficulté une répression féroce. Mais, d'une autre part, il semble pouvoir focaliser l'attention sur des échelles plus modestes, par exemple sur des spécificités locales et régionales, et honorer des revendications, en résonance pour le coup avec l'idée fédérale et le principe de subsidiarité qui veut qu'un échelon subalterne ne doive pas se voir privé du droit d'accomplir ce qui relève de sa compétence propre par un échelon supérieur. Le numérique loin d'infléchir véritablement dans un sens ou un autre l'ordre des choses témoignerait en réalité – tout simplement - des limites d'un ancien état de fait et contribuerait à l'efficacité d'une politique choisie quel que soit le sens où celle-ci s'orienterait. Ainsi, la révolution numérique en elle-même pourrait aussi bien favoriser le dégorgement du centre au profit de la périphérie que renforcer son emprise réelle sur elle. Comme la fameuse langue d'Esope, tout dépendrait en définitive du contexte et de la façon dont le numérique s'avère utilisé. Le choix du modèle à adopter et à entretenir relève ainsi, plus que jamais, du choix politique, mais serait alors confirmé et concrétisé grâce au numérique. Il est intéressant de souligner, d'une part, que le numérique, favorise une

concentration étatique centralisée mais peut aussi, en revanche, redonner de l'efficacité aux échelons plus subalternes. D'autre part, il pourrait correspondre à l'équilibre recherché dans le fédéralisme, limitant les prétentions dangereuses à l'échelon national, et articulant la gestion à petite échelle, avec une indépendance reconnue, et la formation d'une unité différenciée surmontant la tentation du nationalisme.

106. En 1789, il a fallu trois semaines pour que la Franche Comté apprenne la prise de la Bastille. La lenteur de la communication dissuade les volontés d'un pouvoir trop centralisé en raison de la difficulté concrète qu'il rencontre pour imposer ses volontés. C'est d'ailleurs pour cette raison que des historiens comme François Furet ou des philosophes comme Michel Foucault ont mis en cause l'idée souvent entretenue mais fausse d'un ancien régime reposant sur le socle d'un état unitaire et la volonté descendante et applicable à tous d'un Souverain, rompant donc avec une vision simplifiée de ce qui précède 1789[76]. Reprenant des études anciennes, mettant en évidence la grande disparité entre les provinces françaises, ils ont établi que la révolution va en fait introduire une rupture avec un mode de fonctionnement qui met en valorise les régions, et qui n'est pas sans faire penser quelquefois à un état fédéral sans l'adjectif comme le laisse deviner l'historiographie la plus récente[77]. Faute de réaliser un projet unificateur, la royauté d'avant 1789 s'accommode des clivages coutumiers et des frontières internes du royaume[78]. Par la suite, les progrès technologiques semblent favoriser un état unitaire et très centralisé. La décentralisation est évoquée dans les années soixante-dix et quatre-vingt comme un projet de réforme de société mais qui ne tient pas toujours ses promesses, en raison peut-être d'un atavisme institutionnel et administratif[79]. En fait, cette évolution n'est pas aussi tardive que l'année 1982 où elle commence à prendre corps dans la loi du 2 mars, mais traduit un processus ancien. Si la révolution inaugure une volonté de contrôle, dans la volonté d'une division uniforme du pays, si elle substitue aux anciennes provinces marquées souvent par une vraie disparité juridique, au profit des départements qui sont des instruments de centralisation, au fil des décennies, le bienfait d'une certaine décentralisation finit par s'imposer, en particulier à partir du tournant

[76] François FURET, *Penser la révolution française*, Paris, Gallimard, 1978; Michel FOUCAULT, *Folie et déraison. Histoire de la folie à l'âge classique*, Paris, Plon, 1961.
[77] Marie-Laure LEGAY, "La fin du pouvoir provincial (4 août 1789 - 21 septembre 1791), *Annales historiques de la Révolution française*, 332, avril-juin 2003, 25-53.
[78] Jean HILAIRE, "La France méridionale avait-elle une frontière sous l'ancien régime", *bulletin de l'Académie des Sciences et Lettres de Montpellier, 2*008, 45-54.
[79] Patrick LE LIDEC, "La relance de la décentralisation en France. De la rhétorique managériale aux réalités politiques de l'acte II", *in Politiques et management public*, 23, 3, 101-125.

libéral du Second Empire de Napoléon III en 1860[80]. Cette remarque permet de constater l'existence à une même époque de tendances à la fois centrifuges et centripètes. Une évolution n'est jamais absolument à sens unique, un point à garder présent tout au long de notre recherche. Ainsi, c'est par une corrélation assez évidente que la simplification des déplacements et des moyens de communiquer peut contribuer à la réalisation effective d'un dessein centralisateur qu'illustre l'état unitaire. Mais on peut également se demander si la simplification permise ne bénéficie pas à des échelons plus petits. Autrement dit, il n'y a peut-être pas à exclure une sorte d'effet paradoxal, une même cause produisant des effets opposés, par exemple à des échelles diverses : au niveau global et au niveau local. Cela pourrait être le cas, par exemple, du réchauffement climatique. A l'échelle globale la planète se réchauffe, mais ici ou là, localement certains climats évoluent dans le sens du refroidissement. Au plan économique, l'élévation globale du niveau de vie s'accompagne hélas du recul de celui de certains. Selon l'ancienne expression française : l'exception confirme la règle. Mais il faut peut-être aller plus loin et envisager qu'une même cause suscite à égalité deux effets opposés. Par exemple une mesure coercitive pourrait à la fois obtenir l'effet voulu et son contraire en réaction, par exemple la loi sur la prohibition de l'alcool en 1919, ou peut-être des mesures de répression de la prostitution. Ainsi, les nouvelles possibilités offertes par le numérique semble pouvoir bénéficier aussi bien à une centralisation autour de l'état unitaire qu'à une mise en valeur des régions et de leurs compétences autonomes. En fait, le numérique rend possible ce qui ne l'était pas hier mais n'induit pas forcément un modèle constitutionnel et politique totalement déterminé. Simplement, il permet à une ligne adoptée de se poursuivre de façon plus efficace. Il permet une ouverture sur le lointain mais permet de mettre aussi en relief des atouts plus proches. Ainsi, d'une certaine façon, il peut également contribuer à l'implantation ou à la consolidation d'un modèle fédéral, permettant une harmonisation plus rapide et plus juste des différents niveaux de compétence. De toute manière, certaines décisions relèveront toujours de choix politiques et même éthiques ou philosophiques en amont, même lorsqu'ils sont plus implicites que formulés, et non pas seulement de l'influence, pour considérable qu'elle puisse être, des nouvelles technologies. Comme nous l'avons dit plus haut, seul en son genre dans la région, les Emirats suivent un régime fédéral qui tient aussi à leur histoire. Le numérique ne s'y oppose pas de soi, même s'il favorise souvent la centralisation de l'information et des décisions, dans la mesure où

[80] Thomas FRINAULT, "La décentralisation. Retour sur deux siècles de réforme", site metropolitiques.eu, 01/10/2012*, http://www.metropolitiques.eu/La-decentralisation-retour-sur.html*.

il peut aussi contribuer à une harmonisation favorisée et accélérée entre chaque entité fédérée et l'instance fédérale.

107. Il peut être possible de s'avancer davantage et de postuler un lien possible entre la révolution numérique et le fédéralisme en ce sens que la globalisation du monde, devenu village planétaire[81], s'effectue surtout au détriment de l'échelon national mis à mal par la mondialisation mais paraît renforcer l'importance des échelons les moins élevés. En effet, dans un monde qui forme un seul village planétaire, chaque pays semble peiner à conserver son autonomie. En revanche, les spécificités locales et régionales pourraient bénéficier d'un monde globalisé mais qui ne se réduit pas à une pure uniformité. Il y a moins de difficulté sans doute à concilier la suprématie de l'échelle la plus vaste avec la reconnaissance des autonomies locales que d'accorder la globalisation de fait avec les frontières nationales, à dire vrai parfois de nature plus arbitraire qu'impliquée par des identités géographiques ou culturelles bien réelles[82]. Suite à la Seconde Guerre Mondiale, l'humanité semble acquise à l'idée de trouver des regroupements plus larges que les limites nationales, comme l'atteste, notamment le projet de construction européenne, il est vrai d'abord pour éviter une nouvelle guerre européenne, après les meurtrissures des deux grands conflits mondiaux, mais aussi, dans un autre espace géographique, la création de la ligue arabe, peu étudiée et qui accompagne l'émergence d'une identité retrouvée ou composée face à l'émergence d'Israël[83]. Par un effet paradoxal, ce dépassement des frontières nationales par l'élargissement des espaces envisagés favorise aussi la reconnaissance des aspirations et des compétences à l'échelle infranationale. Il y a là une

[81] Marshall McLUHAN*, Message et massage. Un inventaire des effets*, tr.fr., Paris, Jean-Jacques Pauvert, 1968. Le jeu de mot un peu déroutant insiste sur l'effet de masse, à savoir sur la composition d'une masse ainsi unifiée par les nouveaux moyens de communication sociaux. Sans aucun doute, l'idée ne « village planétaire » ne signifie-t-elle aucunement que la planète deviendrait comme un villagge, formant un espace familier et plus humain. Ce que McLuhan établit de façon très solide et aussi prophétique c'est que les nouveaux moyens de communications ne mettent pas seulement en cause les distances inhérentes à un monde de l'écrit mais forge de façon plus rapide une culture de l'immédiateté dans lequel il n'y a désormais plus qu'une seule culture globalisée, vivant au même rythme, s'adonnant à des activités semblables et investissant un même espace. Ce village planétaire se caractérise sans doute par une plus forte interactivité et peut aussi susciter des effets paradoxaux. Le bilinguisme de fait qui tend à s'imposer car chacun doit pouvoir communiquer à la fois dans sa langue propre et dans la langue commune à tous peut induire un renforcement des identités propres par effet de compensation et de réaction. En tout cas, et c'est le point le plus important, tout phénomène social un peu conséquent doit désormais être pensé non seulement localement mais d'abord globalement, ce qui ne veut pas dire toutefois une absorption complète du local dans le global mais son enserrement localement.

[82] La première frontière au sens moderne du terme pourrait avoir été celle tracée le 7 juin 1494 sous la férule dsu pape Alexandre VI et contenue dans le traité de Tordesillas.

[83] Fondée le 22 mars 1945 au Caire, la ligue arabe précède Israël mais non le mouvement de composition de cet état. Son influence réelle demeure limitée au fil des années. Sur ses origines : cf. Robert MONTAGNE, « L'union arabe », in *Politique étrangère*, Paris, 1946, 179-215.

double tendance qui rejoint en définitive l'idéal fédéral renforçant à la fois l'échelon supranational et l'échelon *infranationale*. Ronald Watts le souligne de façon très pertinente : "le fédéralisme permet de concilier ces tendances (apparemment) contradictoires en instaurant un gouvernement commun chargé de poursuivre certains objectifs communs, tout en laissant les gouvernements régionaux mener une action autonome quand des intérêts spécifiquement régionaux sont en jeu"[84]. La révolution numérique qui se joue des frontières conduit à l'affaiblissement d'une vision souverainiste avec, en contrepartie il est vrai, des nostalgies des identités nationales fortes, souvent évanouies, sur le mode d'une sorte de contre-révolution populiste[85]. Cet affaiblissement peut donner le sentiment d'une perte des racines, d'une uniformisation technocratique fortement déshumanisante. Il appelle donc le complément d'un renforcement de l'ancrage à des échelons à taille humaine, ce qui nous semble justement une intuition fédéraliste. Quelquefois il suscite nostalgie et colère pour ce qui paraît avoir été perdu à cause de lui. Les soubresauts divers qui agitent l'opinion politique ne nous semblent pas, à long terme, et sur une longue durée, mettre en cause le changement de paradigme que constitue sans aucun doute l'éclipse des identités nationales que ne dément pas la velléité de les restaurer, qui est plutôt une réaction en bonne part impuissante contre cette nouvelle tendance de fond. Ce changement de perspective se rapproche du modèle fédéraliste puisqu'il traduit un éloignement vis-à-vis d'une conception rigide et étroite de l'instance nationale, seule décisive et décisionnelle, au profit d'une volonté de mettre en place des espaces plus vastes de décision, en équilibre avec les compétences spécifiques des échelons plus modestes[86]. Or cette évolution est à mettre en lien étroit de causalité, ou peut-être d'influence réciproque, avec la révolution numérique.

108. La révolution numérique semble favoriser le regroupement les nouvelles fédérations mais aussi les revendications des entités fédérées. La réciproque paraît également vraie. L'état fédéral favorise la révolution numérique. Pour une raison simple à comprendre : son bon fonctionnement suppose un ajustement permanent et un mouvement de systole et de diastole entre les échelons des deux bouts de la chaîne. Or ils sont beaucoup favorisés, et en partie conditionnés par les atouts du numérique, favorisant la transparence de l'information, la rapidité

[84] Ronald WATTS, "Introduction : le fédéralisme à l'ère de la mondialisation" in *Revue internationale des sciences sociales,* 2001/1, 67, 11 [11-55].
[85] Erwan RUTY, “Le populisme numérique” https://www.cairn.info/revue-esprit-2018-3-p-14.htm
[86] Cf. Daniel Judah ELAZAR, « Fromstatism to federalism : A paradigme shift », *in International Political Science Review,* 1996, 17, 4, 417-429.

des échanges et donc des décisions, sinon prises en commun, du moins harmonisées. En ce qui concerne l'Europe par exemple, malgré le déficit actuel de confiance en un projet fédéral, il ne fait guère de doute que l'harmonisation des décisions, qui évite une perte énorme de temps et d'énergie provoquée par la concurrence ou simplement non maîtrisée entre les états, est rendue possible et améliorée par le développement des nouvelles technologies qui semblent donc particulièrement opportunes. D'une certaine façon, on peut dire qu'il y a une sorte d'articulation trinaire entre le développement technologique, la mondialisation et la valorisation d'un fonctionnement de type fédéral, l'un des phénomènes favorisant l'autre par une sorte de causalité réciproque, de façon assez spontanée, avant même une mise en forme juridique, laquelle risque donc toujours d'être mal ajustée à un existant préalable, et plaqué sur lui. Une évolution profonde est donc en cours, dont il est difficile de dire où elle s'arrêtera, et si jamais elle doit s'arrêter, ce qui est loin d'être immédiat et proche dans le temps. En tout cas les divers niveaux de compétence se structureront de façon différente. Mais avant d'envisager plus avant une telle recomposition et une nouvelle répartition des autorités, dans une perspective opérationnelle, il est peut-être intéressant de repérer les couches du cyberespace comme tel qu'il n'est peut-être possible de transposer comme sur une planisphère mais qui peuvent nous éclairer.

109. Pour filer la métaphore géologique, on pourrait dire que le cyberespace se compose de plusieurs couches, en référence à la fameuse théorie des trois couches[87]. Ces trois couches superposées pourraient être les suivants. En premier lieu, une couche matérielle constituée par tous les périphériques d'accès et toutes les infrastructures nécessaires au fonctionnement. On pourrait parler de l'aspect « physique » d'internet. En second lieu, une couche logicielle avec ses strates propres et tout ce qui permet aux ordinateurs de communiquer les uns avec les autres et d'échanger le plus vite possible. Cette même couche inclut aussi les applications et les programmes plus accessibles ou ludiques. A l'évidence, cette couche est souvent attaquée dans le cadre de la cybercriminalité dont nous parlons plus loin. En troisième lieu, une couche que l'on peut appeler cognitive ou sémantique et qui est en rapport direct et étroit avec le contenu informationnel. Cette couche est aussi celle des interactions sociales les plus fréquentes. Il est à noter que l'on ajoute parfois deux autres couches[88] comme celle de l'infrastructure logique qui comprend tous les services permettant d'assurer la transmission des données ou la couche

[87] Daniel VENTRE, « Le cyberespace définitions, représentations » in *Revue de défense nationale*, juin 2012, 33-38.
[88] Frédérick DOUZET*, op. cit*, 2014.

des applications, la plus simple et la plus familière peut-être à un grand nombre d'usagers puisqu'elle permet à chacun d'utiliser internet sans rien connaître à la programmation informatique.

110. Nous sommes évidemment là en présence d'une conceptualisation théorique du cyberspace. Son objectif et son mérite est de « fournir une dimension géopolitique plus concrète d'internet, c'est-à-dire une certaine forme de matérialisation géographique du pouvoir »[89]. Il va de soi que les Etats-Unis y occupent une place centrale et croissante. Ces nouvelles frontières par leur survenue même contestent les anciennes, impliquent une déterritorialisation et déplacent les limites d'un autre cadastre géographique, politique, humain. En fonction des compétences associées aux possibilités.

[89] Amaël CATTARUZZA, « « Penser l'espace numérique comme un espace stratégique », in collectif*, La cyberdéfense. Politique de l'espace numérique,* Paris, Armand Colin, 2018, 22, [19-25].

Chapitre II : Les meilleurs niveaux de compétence à distinguer

111. Le juriste ne saurait se contenter de prendre simplement acte d'une situation de fait, comme, en l'espèce, la fragilisation des frontières. Il entend redéfinir un cadre devenu obsolète, non pour avaliser forcément un dépassement ou une transgression, mais pour parvenir à une mise en forme plus cohérente. Le juriste se heurte d'emblée à un phénomène que l'on peut qualifier de géopolitique et que Michel Foucher présente comme « l'obsession des frontières »[90]. Ce phénomène est d'ailleurs paradoxal puisqu'il semble contredire l'affaiblissement de la portée des frontières nationales induite par internet. En tout cas, il donne d'ores et déjà confirmation du caractère complexe et à certains égards contradictoire d'une évolution d'ensemble qu'il ne faudrait pas réduire à une seule tendance, tout en se demandant en même temps si des phénomènes qui semblent s'opposer n'obéissent pas d'une part à une logique profonde en amont qui les rend moins contradictoires et d'autre part ne s'inscrivent pas en réalité dans une dynamique d'action et de réaction, certains relevant d'une tendance de fond, et d'autres exprimant une réaction, moins porteuse d'avenir, face aux déstabilisations provoquées par la tendance de fond. Toujours est-il qu'il semble difficile de nier que depuis une vingtaine d'années plus de 30.000 kilomètres de frontière ont été tracées de par le monde. Cette délimitation favorise souvent des conflits, pouvant déboucher sur des affrontements armés. Le morcellement du territoire semble devoir se poursuivre. Ne sommes-nous pas alors contraints de revoir le pronostic optimiste qui associe les nouvelles technologies à la paix dans un monde global pour envisager la manière dont elles risquent au contraire de favoriser d'autres types de conflits et de les multiplier[91]?

112. Il semble par ailleurs certain que notre civilisation ne se fragmente plus en fonction de découpages géographiques et locaux mais se construit et se délimite désormais au travers de réseaux. D'une certaine façon, les réseaux ont toujours existé sous une forme différente il est vrai. Dans l'Empire Romain, par exemple, le clientélisme [92] constitue certainement une forme de sociabilisation séparant ceux qui appartiennent à un réseau constitué par des liens divers de ceux qui, en revanche, n'y participent pas. Ce clientélisme à l'ancienne implique des liens de

[90] Michel FOUCHER*, L'obsession des frontières*, Paris, 3e éd., Tempus Perrin, 2012.
[91] Philippe BOULANGER, *Géopolitique des médias. Acteurs, politiques, conflits*, Paris, Armand Colin, U Science Politique, 2014.
[92] Cf. Elizabeth DENIAUX, *Clientèles et pouvoirs à l'époque de Cicéron*, Rome, Ecole française de Rome, 1993.

subordination assez différents des connections contemporaines en réseau et pourtant on peut dire qu'il les annonce déjà. L'avènement d'une société en réseaux semble irréversible selon l'expression souvent utilisée : « si nous ne nous occupons pas des réseaux, les réseaux s'occuperont de nous ». Et en définitive ces réseaux qui invalident les anciennes frontières vont en créer de nouvelles non plus administratives, territoriales ou locales mais tracées par la maîtrise, ou, au contraire l'incapacité à maîtriser ces nouveaux réseaux. De façon générale, et à plus large échelle, nous ne pouvons pas nous aveugler sur la domination de plus en plus forte du numérique. Celui qui tente simplement d'y résister par une sorte de boycott risque de se retrouver simplement marginalisé.

113. Pourtant, la domination des réseaux se présente, comme l'analyse fort bien Manuel *Castells*[93], de façon paradoxale. Les réseaux font la société mais la société fait aussi les réseaux, les associe ou les oppose, les sélectionne et parfois les cloisonne. De plus, au sein de la société, un nombre croissant de personnes est tenté d'en faire un usage déviant et détourné, à commencer par les hackers. En riposte, les organismes institutionnels traditionnels peuvent retrouver une légitimité renforcée, car ils apparaissent comme des recours face à une déferlante que rien ni personne d'autre ne semble pouvoir maîtriser. Ainsi, dans un premier temps, une société en réseaux fait tomber les frontières, y compris nationales, et contribue à une certaine permissivité. Mais en raison des graves inconvénients qui ne manquent pas de se poser, par un effet de rétroaction bien connu, un phénomène finit par susciter son contraire, et la multiplication effarante du piratage et de la criminalité sur le net provoque en réaction un retour à une volonté de contrôle juridique très contraignant, à partir de délimitations clairement posées, et aussi entretient la nostalgie de frontières nationales plus imperméables. *Castells*, comme d'autres sociologues, s'inquiètent même du risque qui naît de l'adoption de lois visant à contrôler et à assainir internet, en restreignant la liberté, établissant d'autres part une société de la surveillance, et d'autre part de nouvelles réglementations qui enferment. John Perry Barlow, essayiste du courant libertaire, formulait en 1996, une déclaration d'indépendance du cyberespace[94], en réaction contre la volonté de la Maison Blanche d'alors d'établir un contrôle draconien en légiférant de façon détaillée. Ce qui créerait non seulement de nouvelles limitations mais encore un nouveau renforcement de l'institutionnel comme tel et le renforcement des frontières. Pour ce manifeste,

[93] Manuel CASTELLS, *La galaxie internet*, Paris, Fayard, 2001.
[94] Cf. Richard BARBROOK, « La liberté de l'hypermédia – Une réponse à John Perry Barlow » in *Libres enfants du savoir numérique*, Paris, éditions de l'Eclat, 2000.

aucun gouvernement ou entité analogue ne devrait pouvoir s'approprier internet. La déclaration énonce, dans seize paragraphes courts, quelques principes en ce sens soulignant que les États-Unis n'ont pas eu le "consentement des gouvernés" pour imposer leurs lois concernant internet, et ce d'autant plus qu'internet se trouve au-delà des frontières de n'importe quel pays. Toutefois, la théorie la plus importante semble être celle d'une auto-régulation d'internet par lui-même, de senteur typiquement libérale. Au fond, internet lui-même doit trouver et imposer ses propres codes et mettre en place une déontologie et une éthique adaptées à ce qu'il est mais également applicable et largement appliqué. Dans l'esprit de liberté qui lui semble être celui des Pères Fondateurs des States, en particulier Thomas Jefferson, telle lui semble être la seule attitude digne de l'Amérique. Comme on peut l'imaginer, les vues de Barlow ont été largement diffusées sur le net. Du reste, un magistrat virtuel a même été mis en place par l'Institut de droit du cyberespace, désormais hébergé par le "Chicago-Kent *College of Law*". Emerge ainsi, justement, la problématique que doit affronter le juriste : protéger sans enfermer ; contrôler dans une certaine mesure pour empêcher les déviances mais garantir aussi un véritable espace de liberté personnelles. L'entreprise semble ardue, et les choix juridiques qui seront faits sont certainement conditionnés par l'orientation philosophique dominante, qui peut privilégier la liberté, ou à l'inverse, la sécurité. Beaucoup tient dans cette question à la conception que l'on nourrit du rôle de l'Etat ou au contraire des réticences à cet égard[95]. Ainsi, il n'est que partiellement vrai que le numérique, de soi, induisent nécessairement ou presque certaines évolutions juridiques. Il est également vrai que des choix philosophiques et juridiques s'imposent au départ qui vont de toute façon reconfigurer ce nouvel univers du numérique. Ainsi, comme par un processus de systole et diastole, le numérique et le législatif se reconfigurent l'un vis-à-vis de l'autre, ce qui donne toute son importance à la mission du législateur et à ses choix, qui relèvent d'une dimension politique d'administration et d'organisation de la société, en considération d'une certaine vision de départ. Une option fédéraliste sera certainement moins tentée de trop réguler le numérique. En revanche, une volonté de centralisation induira une approche différente, plus suspicieuse au départ, mais aussi récupératrice ensuite, de la dynamique numérique. Dans la recherche d'une solution modérée, on peut estimer qu'en réalité il y a peut-être lieu, à la fois pour ne pas prendre simplement prendre acte de la disparition des frontières et pour éviter aussi de nouveaux déséquilibres, de

[95] Significatif en ce sens : Jean BRILMAN, *La démocratie étouffée par l'Etat. L'étatisme en France*, Paris, L'Harmattan, 2016.

s’interroger sur des niveaux différents de compétence à préciser, pour une délimitation non pas arbitraire mais cohérente, efficace et respectueuse d’une vision politique.

114. En soi, la révolution numérique introduit bien entendu un facteur de concurrence par rapport à l'exercice classique du pouvoir de nature politique. Bien entendu, "le pouvoir politique a tôt saisi la puissance de structuration des sociétés détenue par le monde technico-économique et a tenté d'exercer une emprise tant sur le champ de son action que sur l'axe de ses développements"[96]. Cette subversion de la dimension verticale du pouvoir politique tient en bonne part au fonctionnement intrinsèque du réseau : "un réseau d'égal à égal, avec une certaine symétrie entre producteur de contenu et consommateur"[97]. Cette symétrie rompt avec la dissymétrie fondamentale qui caractérise au contraire l'ordre politique et les instances administratives, sur le modèle d'une hiérarchie souvent pyramidale.

115. La mise en cause des frontières territoriales traditionnelles s'accompagne de la montée d'une nouvelle notion, celle d'"intelligence territoriale", associant précisément de façon ingénieuse les collectivités et les usagers sur un mode non-hiérarchique[98]. Une semblable notion, comme celle de "territoire numérique" du reste semble assez difficile à saisir et porte d'une certaine manière les marques de l'ambivalence qu'elles illustrent. La révolution numérique à la fois dissout le territoire mais en même temps le constitue autrement : "ou bien il s'agit de dissoudre le territoire grâce à la technique, de le "déterritorialiser" au sens où il serait délocalisé dans l'information et le "virtuel", ou bien, en revanche, il s'agit d'enrichir et d'augmenter le territoire à l'aide de réseaux techniques et d'outils logiciels"[99]. On peut voir dans cette alternative deux options fondamentales définitivement opposées par un "oui" disjonctif, mais il nous semble qu'en fait il s'agit de deux mêmes aspects complémentaires, le premier de destruction d'un ordre existant, le second, en revanche de nouvelle construction. En fait ces deux aspects se retrouvent dans tout processus de transformation, en économie ou dans la vie sociale comme l'avait fort

[96] Eric SADIN, *La vie algorythmique : critique de la raison numérique*, Paris, l'Echappée, 2015, 193.
[97] Simon CHIGNARD, *Open data, comprendre l'ouverture des données publiques,* Limoges, Fyp, 2012, 33)
[98] Cf. Mabrouka EL HACHANI, "Open data, collectivités et usagers : une dynamique en question", in *Open data. Accès, territoires, citoyenneté : des problématiques info-communicationnelles,* sous la direction de Françoise PAQUIENSEGUY, Paris, 2016, 1-22.
[99] Pierre MUSSO, "Critique de la notion de territoires juridiques' in *Quaderni, La Revue de la communication*, 2008, 1, 15.

bien compris Joseph Schumpeter théorisant la "destruction créatrice [100]. D'un côté, le territoire se défait mais d'un autre il se constitue autrement, et les deux processus sont davantage concomitants que successifs. De façon plus concrète, ce double processus de décomposition et de nouvelle composition s'inscrit aussi dans des réformes politiques menées, intégrant d'autres phénomènes que nous avons déjà évoqués d'évolution sociale, comme la métropolisation qui honore le rôle moteur des grandes agglomérations. C'est au croisement de diverses évolutions que peut donc s'imposer la notion de "*smart city*" contenant une charge explosive contre un ordre politique figée. Désormais les diverses activités et les différents projets deviennent transversaux. En ce qui concerne par exemple de façon spécifique les données sur un territoire, il s'avère indispensable de mettre en relation des producteurs hétérogènes de données qui rendent d'autant plus nécessaire une plate-forme de base et d'arrivée, ce qui est ainsi le cas dans une ville comme Lyon[101]. Une telle « ville intelligente » utiliserait les nouvelles technologies pour une gestion optimale des données, aussi bien pour gérer les systèmes de circulation et de transport, les centrales électriques, les réseaux d'approvisionnement en eau, la gestion des déchets, les systèmes d'information, que les écoles, les bibliothèques et les hôpitaux. Les gains semblent évident : une meilleure qualité, les performances des services urbains, la réduction des coûts et de la consommation, la multiplication des contacts, la rapidité des interventions ou des décisions. Ce qui fait une ville intelligente c'est précisément un réseau de capteurs sans fil, technologie de pointe qui permet de mettre en place un réseau réparti de noyaux de capteurs intelligents afin de mesurer plusieurs paramètres intéressants en vue d'une meilleure gestion de la ville. Ainsi, à titre d'exemple, les citoyens pourraient-ils surveiller le niveau de pollution dans chaque rue de la ville ou encore recevoir une alerte quand le niveau de radiations atteint dépasse une certaine limite. On peut même envisager des poubelles intelligentes qui informeraient les éboueurs qu'elles sont pleines et qu'ils peuvent – ou doivent – désormais les vider. Les automobilistes peuvent savoir où se garer et trouver une place. Bien entendu, des questions éthiques se posent dans la mesure où la quantité vertigineuse de données recueillies se présente comme vertigineuse. De plus, il est difficile d'identifier la nature des différentes données et ainsi de les classer en données autorisées ou non. Il faudrait aussi déterminer à quelles fins elles sont enregistrées, or il peut certainement y avoir une récupération déviante et inattendue au départ. Mais surtout peut-être, les dispositifs engagés semblent vulnérables et

[100] Cf. Joseph SCHUMPETER, *Business Cycles : a Theoretical, Historical and Statistical Analysis of the Capitalist Process,* New-York / Toronto/ Londres, McGraw-Hill Book Company, 1939. Cf. aussi James M. UTTERBACK, *Mastering the Dynamics of Innovation,* Harvard, Harvard Business School, 1996.

[101] Patricia RAHMé, "Les projets Open data des collectivités territoriales : une analyse des facteurs déterminant le choix de données ouvertes", in *Open data (2016*, cit.), 63-64.

offrir peu de résistances aux attaques des hackers d'aujourd'hui et plus encore de demain[102]. De toute urgence, il importe donc de rendre les smart cities davantage protégées comme entend le faire, entre autres, un Cesar Cerrudo[103].

116. Dans le contexte de la stratégie Europe 2020, une étude s'est intéressée à 468 villes européennes de plus de100 000 habitants, en vue d'opérer un classement selon quatre niveaux de maturité et de développement. Selon le premier niveau, la ville dispose d'une politique ou d'une stratégie de ville intelligente, même à l'état sommaire ou embryonnaire. C'est déjà un début. Au niveau 2, cette politique ou stratégie s'avère déjà plus développée. Au niveau 3, on peut reconnaître des initiatives-pilotes. Enfin, au niveau 4 on peut estimer que la politique de ville intelligente est déjà parvenue à un résultat conséquent. Six villes seulement sont placées dans cette catégorie : Amsterdam, Barcelone, Copenhague, Helsinki, Manchester et Vienne. Mais par ailleurs 90 % des villes européennes de plus de 500 000 habitants sont considérées comme des villes intelligentes. En France, en mars 2016, le Commissariat Général au développement durable publie une étude remarquée sous le titre « Villes intelligentes, smart, agiles, enjeux et stratégies de collectivités françaises ». Elle dégage deux objectifs principaux : d'une part, une opportunité de développement économique local et, d'autre part, une optimisation des services. Quelques semaines plus tard, un livre blanc sur le thème « Le numérique et la ville » est composé par trois pôles de compétitivité franciliens (*Advancity, Cap Digital et Systematic Paris-R**egion***) regroupant plus de 1500 entreprises et 200 établissements d'enseignement supérieur et de recherche. Il s'agit, entre autres, de jeter des passerelles entre acteurs publics et jeunes entrepreneurs privés.

117. Dubaï, dans les Emirats, entend bien devenir une cité intelligente elle aussi. Cela passe pour elle des voitures intelligentes aux bornes Wifi et aux applis de localisation publication, mais aussi à de nouveaux dispositifs policiers de contrôle. De façon un peu pittoresque, on peut signaler le palmier intelligent, émetteur de Wi-Fi et chargeur de téléphone. Haut de six mètres, il capte et canalise l'énergie solaire, très abondante à Dubaï en considération du climat que l'on sait. Cette énergie en abondance permet de fournir des bornes Wi-Fi gratuites, des ports pour charger les téléphones et d'autres gadgets, ainsi que de communiquer des informations météo

[102] Par exemple *: https://www.tomsguide.com/us/hackers-smart-town,news-20822.html*
[103] *https://threatpost.com/cesar-cerrudo-on-securing-smart-cities/115023/*

ou touristiques, toujours à partir du tronc de ce palmier. Il existe plusieurs palmiers de ce type sur la plage Kite Beach et dans le parc Zabeel, sans compter ceux encore en projet d'installation. Ville passée rapidement à une sorte d'ultra-modernisé, Dubaï n'est pas propice à la circulation déjà en raison des déficiences de la signalisation et de la numérotation des rues. Pour faciliter le suivi des itinéraires et donc une circulation plus fluide, un nouveau système révolutionnaire a été mis en place. Un numéro unique a été alloué, clairement affiché à chaque édifice de l'émirat, utilisé déjà par les services d'urgences ou les véhicules de livraisons, mais qui devrait élargir son champ d'application. De nombreuses applications rendent la vie des visiteurs à Dubaï plus simple. Ainsi, l'appli Dubaï Tourisme App propose-t-elle un guide complet des choses à faire dans la ville, sans oublier les restaurants ou les lieux à découvrir. La plupart des centres commerciaux les plus importants, tel le centre commercial de Dubaï, le Mall of the Emirates et le centre commercial de la marina de Dubaï, disposent déjà de leur propre application. Ces diverses applications très au point aident les visiteurs à trouver les boutiques recherchées et à explorer les diverses offres de shopping et de divertissement. Ce système inclut un navigateur GPS Garmin permettant de trouver facilement une adresse et de la rejoindre en voiture. Une attention particulière doit en outre être accordée au plan « Dubaï Smart City 2021 » et à la stratégie fédérale pour l'Intelligence Artificielle, lancée en Octobre 2017, dont la contribution s'avère considérable bénéfique au développement d'une économie numérique. Bien entendu, dans cette mouvance technologique, les incubateurs et les accélérateurs de start-ups ainsi que les *co-working* espaces deviennent incontournables, et les zones franches spécialisées (Dubaï Internet City, Dubaï Silicon Oasis) facilitent la transformation digitale du pays qui s'accélère de jour en jour. On est également en mesure de citer notamment le programme d'accélération « The Greenhouse », mené par le groupe Chalhoub, leader de la distribution de marques de luxe dans la région. Les investisseurs locaux, régionaux et mondiaux se montrent de plus en plus attentifs à ces programmes. Des objets connectés (Iot) à la Fintech en passant par la *RetailTech*, l'E-commerce, la Cybersécurité, la Blockchain, l'Intelligence artificielle ou encore la réalité augmentée et virtuelle, Dubaï s'ouvre au monde pour rechercher des start-ups répondant aux besoins de la ville, moderne et innovante.

118. Ainsi, une ville intelligente, permet-elle de mieux coordonner divers services. Les niveaux de compétences à déterminer constituent un problème juridique de première importance, qui oriente également les choix à faire en matière d'organisation politique et institutionnelle. Le fédéralisme lui-même dont nous avons amplement parlé se présente comme une application du

principe de subsidiarité[104] pour lequel la responsabilité d'une action incombe à l'entité institutionnelle dont c'est la compétence spécifique, à l'échelon qui convient. Le principe de subsidiarité répudie aussi bien la tentation d'une sorte de sous-traitance généralisée, l'échelon compétent n'intervenant pas et laissant cette tâche aux échelons subalternes, et celle d'une concentration indue des pouvoirs par les échelons supérieurs privant des entités subalternes de l'autonomie propre et de la responsabilité qui est pourtant la leur. L'affirmation du principe de subsidiarité, depuis Johannes Althusius au début du XVIIe siècle, mais en référence à la théologie médiévale plus ancienne, s'inscrit dans un contexte, celui d'un ordre naturel qu'il serait malheureux de contrarier en privant l'entité compétente de son droit d'exercer la responsabilité pour laquelle elle est faite. Mais il peut aussi servir la cause d'une citoyenneté véritable, car il s'oppose à ce qu'une instance compétente se voit privée de ses responsabilités par des échelons supérieurs concentrant ainsi tout pouvoir dans un schéma vertical très peu démocratique. Du reste, les différentes enquêtes faites sur l'opinion témoignent bien de la difficulté des gens à accepter que des instances hiérarchiques prennent en fait les décisions qui leur incomberaient, et les spolient de leur faculté d'initiatives et de décisions. Ce sentiment a pu émerger en France lors de la crise sanitaire du Covid-19, par exemple au sujet du manque de masques ou des règles du confinement, identiques dans un département avec de forts cas de contamination et dans des départements préservés comme la Lozère ou le Cantal, où il semblait absurde de se voir interdit de se promener en forêt. Dans d'autres cas, la motivation pragmatique, considérant en quelque sorte l'efficacité et le rendement, est comme seconde par rapport au choix que l'on pourrait qualifier d'axiologique. En effet, ce n'est pas tant en raison d'une utilité pratique que l'on peut parfois contester que s'impose la subsidiarité mais pour des raisons idéales, avant tout philosophiques, ou même théologiques, dans la mesure où elle semble un corrélat obligatoire aussi bien d'une vision religieuse pour laquelle l'organisation de la société et des pouvoirs doit correspondre à un dessein divin que d'une volonté d'étendre la démocratie, les deux perspectives n'étant d'ailleurs pas contradictoires, comme le suggère le modèle américain[105]. Mais les deux types de considérations, axiologique et pragmatique, irréductibles l'une à l'autre, et possiblement en conflit, ne le sont pas forcément, et peuvent faire l'objet d'un ajustement réciproque, dans le compromis. Ceux deux motivations rationnelles de l'agir humain sont en fait plus complémentaires qu'opposées, et aucune d'entre elle ne semble suffisante à rendre compte des choix rationnels de l'homme et de l'humanité, comme l'a mis en valeur le

[104] Sur le principe de subsidiarité : Jean-Louis CLERGERIE*, Le principe de subsidiarité*, Paris, Ellipses, Paris 1997.
[105] Cf. les justes remarques de Raymond BOUDON, *Tocqueville aujourd'hui*, Paris, Odile Jacob, 2005.

sociologue Raymond Boudon[106]. La perspective qui est spécifiquement la nôtre se veut et se doit d'être quelque peu différente car elle entend faire le lien entre le développement numérique et le choix de l'organisation politique, aussi bien sous l'angle théorique idéal que sous l'angle plus pragmatique d'une culture du résultat, indispensable pour la bonne santé économique.

119. La division des compétences est un problème aussi ancien que l'humanité. Dante Alighieri au XIVe siècle, dans sa *Monarchie,* suggère le choix d'un tel régime justement pour ne pas diviser les compétences, ce qui risque toujours de susciter tensions et conflits. Dans son énonciation sommaire, le principe de subsidiarité postule que le niveau compétent doit se voir respecter sa propre responsabilité. Reste à savoir qui peut la définir : lui-même? D'autres? Une instance supérieure? Une majorité électorale? L'affirmation du principe de subsidiarité semble quelquefois relever de la pétition de principe, car la délimitation de la compétence n'est pas toujours évidente, et le devient de moins en moins, dans la mesure où dans un véritable village planétaire, celui de la mondialisation, l'imbrication réciproque devient la norme, de sorte qu'il parait de plus en plus difficile de prétendre qu'une décision n'aura qu'une implication limitée et clairement circonscrite. Ainsi, loin de se présenter comme une sorte de clé universelle résolvant tous les problèmes, le principe de subsidiarité peut sans doute constituer un axe mais qui n'évacue pas un discernement délicat présidant à la répartition des compétences. Toute constitution, au demeurant, veille à répartir le champ de compétences des responsables, comme entre le président de la république et le premier ministre en France, depuis 1958, dans le sens d'un équilibre propre à un régime en fait semi-présidentiel. Très souvent, la délimitation est à la fois facilitée et rendue plus complexe par la dimension géographique et territoriale. Une politique de décentralisation, par exemple, qui délimite la compétence d'un ministère et du président de région entre autres, souligne l'importance du territoire, pour une décision adaptée : l'échelon local étant davantage en prise avec les réalités de terrain mais manquant quelquefois de recul, et de sensibilité à l'impact ailleurs d'une décision prise localement. La révolution numérique, nous l'avons dit, a une incidence paradoxale. D'une part, elle favorise la concentration des pouvoirs et des décisions; de l'autre elle hisse chaque échelon au niveau d'information et de communication qui lui permet d'agir. Ainsi le problème de la délimitation

[106] Cf. Raymond BOUDON, *Déclin de la morale ? Déclin des valeurs* ? Paris, PUF, 2002 *; Y a-t-il encore une sociologie* ?, Paris, Odile Jacob, 2003 (entretiens avec Robert LEROUX) ; *Raison, bonnes raisons*, Paris, PUF, 2003 ; *Renouveler la démocratie : éloge du sens commun*, Paris, Odile Jacob, 2006 ; *Essais sur la théorie générale de la rationalité*, Paris, PUF, 2007 ; *La rationalité*, Paris, PUF, coll. « Que sais-je ? », 2009.

des niveaux de compétence se présente-t-il comme aussi délicat qu'incontournable, en considération de la révolution numérique.

120. Au niveau des compétences institutionnelles, la distinction doit être faite en fonction de la légitimité à agir d'une façon ou d'une autre. Mais la reconnaissance d'une compétence pour agir renvoie à la question de la légitimité de la connaissance, autrement dit du droit éventuel de posséder une information. Le phénomène des *open data*, à savoir des données le plus largement connues, semble répondre à un droit de chacun à être informé de tout ce qui le concerne, voire de ce qui concerne les autres, hormis ce qui relève de la sphère proprement privée, d'ailleurs éventuellement menacée, et certainement à définir. Nous revenons sur ces problèmes plus loin mais ils se posent déjà dans la question de la délimitation d'une compétence décisionnelle qui est aussi la délimitation d'un droit à être informé, peut-être plus vaste et moins spécifique. On peut d'ailleurs se demander jusqu'où la simple condition de citoyen ne fonde pas un droit à être tenu informé qui n'implique cependant pas une compétence immédiate dans l'ordre décisionnel. Néanmoins dans la mesure où la démocratie se définit bel et bien comme un régime dans lequel le peuple est souverain et jouit au fond du pouvoir, même s'il est exercé concrètement par d'autres, en particulier dans le cadre d'une démocratie représentative, elle semble impliquer un droit du peuple, et donc de chacun, d'être informé de son sort pour pouvoir en décider. La question de la délimitation des compétences se présente donc comme différente du droit d'être informé mais aussi comme étroitement reliée à ce dernier, qu'elle suppose. Toute prise de décision suppose en effet d'être informé. La réciproque n'est pas vraie, toutefois. On peut disposer du droit d'être informé, sans avoir le droit d'intervenir et de prendre une décision, même si disposer de l'information semble conférer de fait, avant la reconnaissance juridique, d'un certain pouvoir, tant le savoir et le pouvoir sont articulés comme le souligne par exemple le philosophe Michel Foucault [107]. Il n'empêche. Du point de vue juridique qui est le nôtre, tout organigramme institutionnel semble devoir non seulement délimiter les compétences décisionnelles mais aussi le droit à être informé, qui peut aussi s'exercer de façon négative, comme un savoir réservé et interdit à d'autres, par exemple pour des raisons de sécurité. Un droit spécifique à être informé, par exemple de secrets militaires, est étroitement connexe à des décisions à prendre, qui relèvent d'une compétence particulière, souvent exclusive.

[107] Cf. Michel FOUCAULT, « Espace, savoir et pouvoir », entretien avec Paul Rabinow, Skyline, mars 1982, 16-20 *; La volonté de savoir*, Paris rééd., 1994, Paris, Gallimard, collection « tel ».

121. Se pose alors la question des experts, de ceux qui savent, mais en principe ne décident pas et se contentent de conseiller ceux qui légitimement prennent des décisions. L'histoire universelle abonderait d'exemples de conseillers qui en fait prennent les décisions que les autorités légitimes se contentent de suivre et d'avaliser. En ce qui concerne des questions très pointues, l'expert est riche, qu'on veuille bien le reconnaître ou non, du vrai pouvoir de décision car l'autorité compétente n'a pas une connaissance (ou une compréhension) suffisante d'une question. Tout le monde connaît le film célèbre de Stanley Kubrick, le Docteur Folamour, qui présente un expert pervers et psychopathe, mais dont le point de vue l'emporte de toute façon dans la mesure où il est "supposé savoir". Des décisions prises par des experts sans consultation populaire ne trahissent-elles pas la démocratie? Mais comment le peuple peut-il vraiment trancher certaines questions et prendre certaines décisions complexes, dont la simple compréhension relève d'une formation poussée et technique? On se souvient du référendum sur la constitution européenne soumis aux électeurs français en 2005, sous forme d'un projet de traité opaque à la lecture, même attentive. Bien entendu, chaque électeur est en mesure de faire un choix entre un renforcement de la dynamique fédérale ou au contraire un ralentissement. Quant à évaluer de façon précise les différents points, leurs tenants et aboutissants, cela semble relever d'une compétence technique, elle-même fragile tant des hypothèses variées et contradictoires peuvent avoir cours, par exemple quant aux conséquences économiques d'un ralentissement de la construction européenne. La sauvegarde d'une véritable démocratie n'implique-t-elle pas de se défier d'une emprise des experts? Mais peut-on ignorer la complexité des enjeux et des décisions pour sauver la démocratie, au risque d'éluder les vraies questions et de trancher à l'aveugle? Il semble que la réponse à cette alternative puisse justement résider dans une politique d'information mais également de formation, dans la mesure où une donnée ne doit pas simplement être accessible mais compréhensible, sans quoi l'information est fallacieuse et confine à la désinformation. Il est certain que la situation actuelle présente une singularité étonnante par rapport aux périodes passées. Celle d'un accès très facile à l'information, celui dont jouit la génération de la « petite Poucette" dont parle Michel Serres [108]et qui jouit potentiellement d'un savoir considérable. Néanmoins, la masse de savoir peut entraîner à la confusion, et, de plus, l'avancée de certaines connaissances est telle qu'il faut parfois une formation poussée pour y voir clair, de sorte que la situation actuelle est irréductible à une simple facilitation dans l'acquisition des connaissances et des informations, car plus les

[108] Michel SERRES*, Petite Poucette*, Paris, Le Pommier, 2012

moyens de connaître se développent, plus ce qui est à connaître devient complexe. Ainsi, le rôle des experts, déjà anticipé par exemple par celui des clercs du Moyen Age qui avait accès à des connaissances en quelque sorte réservées, ne cesse de grandir, sous une autre forme il est vrai. Toute délimitation des compétences institutionnelles ne peut en faire fi, mais ne peut non plus abdiquer sa responsabilité face au constat de fait d'une influence considérable de celui qui dispose d'un savoir non accessible à d'autres, même et surtout s'il l'est techniquement (grâce au numérique par exemple) mais non de facto faute de formation et de capacité de l'assimiler.

122. La nouvelle délimitation des compétences institutionnelles ne peut simplement exprimer une aptitude plus ou moins grande de fait à aborder et à comprendre les nouvelles technologies, ce qui reviendrait à une absorption de la légitimité politique et institutionnelle par le savoir technique, créant ainsi une oligarchie, même inavouée, contraire à la démocratie. En d'autres termes, si la nouvelle distribution des compétences institutionnelles ne peut ignorer l'impact de la révolution numérique, elle n'en est pas la pure et seule application au plan institutionnel mais s'inscrit dans une visée spécifiquement politique. Ainsi, paradoxalement, la domination accrue des nouvelles technologies appelle une nouvelle reconnaissance de la dimension politique comme irréductible à une pure combinaison pragmatique et comme étant finalisé par un projet préalable, en l'occurrence de renforcement de la démocratie. En France, par exemple, cette perspective politique s'inscrit dans une constitution qui offre non seulement une sorte d'organigramme institutionnel mais encore un cadre global, y compris théorique. En effet, la constitution de 1958, norme juridique ultime, contient un préambule renvoyant à deux textes fondamentaux "la déclaration des droits de l'homme et du citoyen" du 26 août 1789 et le "préambule de la constitution du 27 octobre 1946", auxquels s'ajoute la Charte de l'environnement de 2004. Ces textes forment ce que l'on appelle quelquefois avec raison "le bloc de constitutionnalité" posant les principes de toute organisation de la France, et donc de la délimitation des compétences. Dans les Emirats Arabes Unis, la constitution de 1971, devenue permanente en 1996, prenant acte d'un regroupement d'entités fédérées, et désireuse de la consolider et de la protéger, veut permettre au peuple de mener "une vie constitutionnelle libre et digne", en optant pour "un régime démocratique pleinement achevé", avec cette spécificité : "dans le cadre d'une société arabe et islamique libérée de la peur et de l'inquiétude" L'objectif souligné est que le pays puisse "occuper une place de choix parmi les Etats et les nations les plus civilisés". Il semble donc particulièrement clair qu'il ne s'agit pas simplement d'enregistrer

des évolutions technologiques mais de les intégrer dans un projet qui fait sens et incarne une vision politique. Un projet global et complexe.

Section I : La concentration et la décentralisation de l'information à l'ère du numérique.

123. On ne peut nier que le numérique favorise, nous l'avons relevé plus haut, une tendance à la concentration des pouvoirs. Il est possible de concevoir cette dernière comme étant l'ennemie irréductible de toute subsidiarité au service de l'ambition d'un seul, personne physique ou morale, mais on peut également la concevoir comme une tendance qui appelle et complète la tendance opposée, comme un mouvement de systole et de diastole. A l'évidence, la concentration de l'information en un lieu central et unique constitue bel et bien une opportunité extraordinaire dont prit conscience Philippe Auguste en 1194, lorsqu'il perdit ses archives, jusqu'alors transportées fort imprudemment avec son armée, à la bataille de Fréteval ce qui le décide à fonder à Paris un dépôt permanent d'archives, auquel tout le monde peut se référer. Ce projet de concentration du savoir, dont l'utilité théorique mais aussi pratique pour prendre quelque décision que ce soit à tous les niveaux parait relever de l'évidence, est assurée par la révolution numérique.

124. Cette concentration du savoir ainsi regroupées et non plus éclaté n'implique pas de façon nécessaire une concentration des décisions. Elle est cependant indispensable, en particulier de deux points de vue. D'une part, elle favorise l'information et l'instruction. D'autre part, elle permet un service de renseignement véritablement efficace. En France, par exemple, les archives nationales ne conservent pas moins de 153.500.000 fichiers soit 35 To de données accessibles, garantissant ainsi l'intégrité, l'authenticité et la disponibilité des archives nativement numériques. Il serait ridiculement absurde de vouloir répartir ces archives. L'accroissement du nombre de ces archives se poursuit bien entendu de façon exponentielle. Il existe aujourd'hui en France un projet *ADAMANT* (Administration des Archives et de leurs métadonnées aux Archives Nationales dans le temps) en vue d'adapter les outils, les procédures et l'organisation de la chaîne archivistique pour répondre aux enjeux numériques actuels. L'effort à fournir est bien entendu important mais également très prometteur car il favorise en retour la facilité de conservation et de consultation, ce qui reste l'objectif associé de toute conservation archivistique, dans la perspective du service public. *ADAMANT* exprime une stratégie d'ensemble visant à améliorer l'ensemble du dispositif de gestion des archives numériques, aussi les bien les infrastructures matérielles que les outils logiciels et les ressources humaines. Tout cela pour garder plus sûrement et plus longtemps des archives et en permettre une consultation accélérée et simplifiée. L'exigence se présente donc comme qualitative comme

l'atteste l'acronyme ingénieux *ADAMANT* qui renvoie aussi au mot anglais exprimant la solidité et l'inaltérabilité. Assez récemment, en France, a été inauguré en 2013 par le Président François Hollande, le site archivistique de Pierrefitte-sur-Seine, en banlieue parisienne, et relativement bien accessible du centre par les transports en commun, non seulement en raison des risques encourus par la conservation au centre de Paris, à l'hôtel de Soubise, avec par exemple un risque non négligeable d'un incendie destructeur mais en vue d'une refondation complète des Archives nationales. La quasi-totalité des instruments de recherche doit être disponible sur l'Internet, de sorte qu'à la concentration de la conservation s'ajoute une concentration sur la toile en préparation à l'éventuelle consultation.

125. Il est intéressant de se souvenir que la loi fondatrice des Archives nationales en France, en 1790, s'inscrivait dans une optique clairement citoyenne. Celle d'accueillir des archives « papier » mais aussi, dans une logique muséale et patrimoniale les objets fondateurs de la République, tels que les sceaux, les étalons des poids et mesures. Aux yeux de la Révolution, les manuscrits et imprimés relatifs aux sciences et aux arts, pouvant et devant contribuer à l'instruction de tous, sont davantage du ressort des bibliothèques, et en particulier de la bibliothèque, créée au départ comme une agence temporaire de tri. En fait, c'est François 1er qui institue en 1537 par l'édit de Montpellier y afférant le dépôt légal, où chaque publication doit être envoyée, placée ensuite sous l'autorité d'un libraire du roi, le premier étant Guillaume Budé et le dernier Malesherbes. La révolution interrompt un temps l'idée d'un dépôt légal qui lui semble relever de l'ancien régime et de l'arbitraire, avant de créer un dépôt facultatif. Ce dépôt légal ou facultatif correspond exactement à l'idée d'une concentration, qui favorise sans doute le contrôle mais évite aussi la dissémination des œuvres qui favorise leur oubli. C'est Napoléon en 1810, par le décret du 10 février qui rétablit le dépôt obligatoire. Depuis, ce dépôt légal s'est étendu aux photographies, au multimédias et à l'audiovisuel. Au niveau international, le portail européen des archives, projet cofinancé par la Commission européenne, permet aujourd'hui de consulter environ 120.000 inventaires de 89 services d'archives répartis dans seize pays, dont la France qui a largement contribué à sa construction. Les frontières sont ainsi dépassées ce qui confirme ce que nous avons souligné précédemment, de sorte qu'il est possible de consulter des archives d'un bout à l'autre de l'Europe. L'idée avance d'archives mondiales, par exemple intéressant les généalogistes, pour des raisons parfois étonnantes comme la volonté des mormons de baptiser les morts ce qui exige de les retrouver – généalogiquement bien entendu – de sorte qu'ils microfilment les archives.

126. La concentration de l'information pose toujours historiquement un problème : celui de sa vulnérabilité. Pour se prémunir d'un voleur, le voyageur avisé sait bien qu'il est quelquefois prudent de ne pas se promener avec un seul sac bien visible, facile à arracher, dans lequel aurait été placé tout l'argent, mais qu'il vaut mieux cacher ce dernier en différents endroits. Le danger perçu par Philippe Auguste d'une destruction des archives est toujours réel, même si le contexte a changé et les moyens aussi. C'est d'ailleurs la tragédie de toutes les guerres qui menacent le patrimoine et l'information souvent regroupée. En réalité, on peut palier à cet inconvénient par des copies, qui se trouvent en différents endroits, mais dans une époque de terrorisme, par exemple, la concentration des données peut constituer une cible privilégiée. Mais ce danger se double de celui, qui concerne surtout le deuxième volet que nous allons étudier, de violation de la confidentialité de certaines archives et des données collectées par les services de renseignements. Au demeurant, en France, certains fonds d'intérêts nationaux sont conservés dans deux autres services que celui de Pierrefitte : les Archives nationales d'outre-mer à Aix-en-Provence (archives des colonies) et les Archives nationales du monde du travail à Roubaix (archives privées d'entreprises et d'associations). En outre, les ministères de la Défense, des Finances et des Affaires étrangères ont leurs propres services d'archives depuis le XVIIIe siècle, appelés respectivement service historique de la Défense, archives économiques et financières et archives diplomatiques. Enfin, on ne saurait négliger l'importance des services d'archives déconcentrés.

127. Ainsi, les archives départementales collectent et tiennent aussi à disposition du public des documents produits par des services de l'État dans le département. De plus, suite aux différentes phases de décentralisation, certaines compétences ont été transférées de l'État aux collectivités territoriales. En tout cas, la réforme générale des politiques publiques a modifié en profondeur l'organisation des services déconcentrés de l'État dans les départements. Il est assez logique, en réalité, que les archives se trouvent non loin de l'endroit où les décisions ont été, et seront prises. L'idéal de la concentration ne saurait occulter la fonctionnalité d'archives qui est évidemment plus forte sur place.

128. La concentration de l'information revêt une dimension particulière lorsqu'il s'agit de données confidentielles, liées au renseignement, qu'il soit civil ou militaire, et dont la qualité est

déterminante pour le travail de police et pour assurer ainsi la sécurité face aux différents types de criminalité. En France, les renseignements généraux créés en 1907, et demeurés légendaires, ont pour objectif principal de constituer une source d'informations concentrée afin de renseigner le gouvernement en place, informations bien entendu secrètes et confidentielles. Curieusement, dans un but de rationalisation, il a été opéré en 2008 une déconcentration dans la mesure où une partie de ses prérogatives a été confiée à un autre organisme, la nouvelle Sous-direction de l'information générale (SDIG), créée au sein de la direction centrale de la Sécurité publique (DCSP), la branche « courses et jeux » des RG étant, quant à elle, transférée à la direction centrale de la Police judiciaire (DCPJ). En France, cette réforme de 2008 est l'objet de très vives critiques précisément en raison de la dispersion des effectifs qui semble offenser le bon sens rationnel, et du reste nombreuses sont aujourd'hui les voix, y compris, le journal satirique, *Le Canard enchaîné* qui appellent de leur voix le retour des anciens renseignements unifiés, même sous une forme différente, forcément modernisée. En attendant, cette modernisation, gage de succès futurs, constitue aussi une difficulté, car elle exigerait un progrès de la maîtrise et de la connaissance de la part de qui se sert de nouveaux logiciels. Il faut savoir, exemple significatif, que les services de renseignements sont encore en août 2017 incapables de se servir de *l'l'IMSI-catcher* acquis pour près de 15 000 euros, et qui contrôle en particulier le trafic des communications mobiles voire capter des conversations ce qui n'est pas sans poser des problèmes éthiques au demeurant, bien que le procédé soit légal depuis 2015.

129. Par ailleurs, l'exigence de concentration est singulièrement forte pour tout ce qui concerne le secret Défense. En fait, la délimitation des documents secrets de ce type telle qu'exprimée dans la loi n° 78-753 du 17 juillet 1978 *portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal* est assez floue, comme de même le secret diplomatique, ce qui n'est pas sans poser un problème, de cadastre immatériel de l'information, pour déterminer ce qui relève de tel champ ou de tel autre, sans oublier que des documents peuvent gagner de l'intérêt pour la défense qu'il n'avait pas auparavant et donc changer de catégorie. Ce qui nous intéresse davantage est la concentration indispensable des informations. On sait qu'en 1940, l'une des causes de la piteuse déconfiture française face aux Allemands fut justement le manque de coordination et d'information, avec un généralissime se trouvant qui plus est hors de Paris, à Vincennes.

130. Le problème de la conservation et de la facilité se croise avec celui, essentiel dans le cas d'espèce, de la protection. Ce n'est pas seulement d'une destruction accidentelle ou criminelle dont il faut protéger les documents mais du viol de leur confidentialité, par exemple par une puissance étrangère ou par des terroristes. La concentration de l'information expose, semble-t-il, à des conséquences beaucoup plus grave en cas de violation de la protection alors que la dispersion ne présente que des risques limitées quant à l'étendue des conséquences mais, en revanche ne permet pas aussi facilement une protection forte en raison justement de la dispersion des éventuels points à attaquer. Une fois traitée la question de la concentration et de la déconcentration des fonds d'information de nature variée, il faut se poser la question qui n'est pas exactement analogue de la concentration ou de la déconcentration des échelons de décision. La concentration semble présenter l'avantage de la rapidité et de l'efficacité à l'échelle globale, tandis que la décentralisation semble davantage coller aux réalités locales ou régionales et apporter une réponse appropriée. Telle est au demeurant la conviction qui préside au principe de subsidiarité qui n'est pas seulement adopté pour des raisons que l'on peut qualifier d'axiologiques, parce qu'il honore mieux :la responsabilité citoyenne, mais aussi pour une action plus rapide et plus pertinente à une échelle plus réduite.

131. Lorsqu'on évoque la question de savoir qui décide dans les Emirats, il est tentant mais simpliste de répondre purement et simplement les cheikhs. Dans le monde occidental, la tyrannie est jugulée par la distinction des pouvoirs et la répartition des compétences, depuis Montesquieu et le onzième livre de son célèbre *De l'esprit des lois*, la démocratie est assurée en France par une division du pouvoir décisionnaire[109]. Dans le cas des Emirats c'est un peu différent car l'arbitraire de la tyrannie est en substance conjuré par l'objection fondamentale qui incombe à tout chef de consulter le plus largement possible, et d'écouter les avis divergents. En regard du potentiel très inégal entre les différents Emirats fédérés, il semble judicieux de placer le projecteur de façon spécifique sur Dubaï. Sans aucun doute, l'affirmation assez forte du principe d'autorité est tempérée par un v rai pragmatisme et une confiance dans le marché et dans ses acteurs. Le monde de l'entreprise y contribue aux décisions politiques[110]. Il faut dire que dès avant le développement de l'économie perlière, les chefs de tribus composent bien entendu avec les commerçants. Les clients sont aussi des partenaires, sans qu'il y ait en

[109] Cf. Michel TROPER, *La Séparation des pouvoirs et l'histoire constitutionnelle française*, Paris, LGDJ, 1980.
[110] Cf. Martin HVIDT, « Public-private ties and their contribution to development. The case of Dubai » in *Middle Eastern Studies*, 43, 4, juillet 2007, 557-577.

définitive besoin de définir en amont le type de consensus souhaité dans la prise de décision, l'approche des émirats étant assez pragmatique. En tout cas, les avis extérieurs autorisés se font entendre même dans le *Majlis*, le conseil de famille jadis réservé aux chefs de la tribu. Là encore, les Emirats entendent rester fidèle à leur volonté foncière d'équilibre entre le poids respecté de la tradition et la souplesse pratique en vue de l'avenir. Ainsi, les cheikhs gardent bel et bien les pouvoir de décision mais ajustent leur sens de l'autorité aux circonstances ainsi qu'aux revendications des différents partenaires. William Guéraiche parle en référence au XVIIIe siècle occidental de « despotisme éclairé » [111].Les décisions sont orientées in fine par des personnes fort compétentes qui forment le premier cercle autour du chef, en évitant la pesanteur institutionnelle et l'embrouillamini administratif. Ce fonctionnement concret, souple et toujours en voie de nouvel ajustement, associe bien le sens des décisions institutionnelles à une sensibilité au terrain, et à la réalité économique du moment, grâce aux choix judicieux des personnes d'influence : « Ces hommes, et quelques très rares femmes, réputé pour leurs capacités et leur fidélité, ont la capacité d'orienter le développement économique parce qu'ils se trouvent aussi à la tête d'un immense patrimoine d'entreprises semi-publiques » [112]Le lien entre Dubaï et la compagnie *Emirates* est connu partout. Le bras armé de cet Emirat est bel et bien formé de très grandes entreprises. On peut dire de façon très intuitive que les Emirats veulent mettre en place une société de la confiance, dont les mérites ont souvent été théorisés [113]. Le succès des Emirats tient en bonne part, il faut le répéter à l'idéal d' »un régime démocratique représentatif dans une société arabe et islamique, libre de toute peur et de toute anxiété »[114]. Autrement, dit pour les Emirats, la vraie et première question du discernement des prises de décision est la confiance. Bien entendu, comme dans le cas des autres pays, les Emirats spécifient également la nature et l'étendue des pouvoirs des responsables de l'exécutif dans la constitution. Le président et le vice-président se voient attribuer des compétences bien clarifiées par les article 51 et 53 de la constitution. Ainsi, en qualité de chef de l'exécutif, le Président préside-t-il les réunions du Conseil Suprême, du Conseil des Ministres et commande-t-il les forces armées. Il lui revient de nommer le Premier Ministre et le Président de la Cour Suprême fédérale. Pour des raisons qui tiennent à la grande disparité entre les Emirats, de taille et de

[111] William GUERAICHE, 2014, 95.
[112] William GUERAICHE, 2014, 95.
[113] Alain PEYREFITTE, *La société de la confiance. Essai sur les origines et la nature du développement*, Paris, Odile Jacob, 1995 ; Gilles LE CARDINAL, « La confiance au fondement de la société », in *Projet,* 293, 2006 / 4, 65-71.
[114] Ibrahim ABED, « The historical background and constitutional basis to the federation », in Ibrahim ABED et Peter HELLYER (dir.), *United Arab Emirates. A New Perspective*, Londres, Trident Press, 2001, 134 [121-144])

richesse différentes, la magistrature suprême est assumée par le cheikh d'Abou Dhabi tandis que la fonction de Premier Ministre revient à celui de Dubaï. Quant à la désignation quelquefois assez mystérieuse d'un prince régnant, elle relève à la fois d'une succession par ordre de primogéniture et du choix par le souverain régnant de son successeur, comme cela existait dans l'Empire Romain naguère, sinon d'une sorte de consensus collégial qui doit se réaliser, à l'exemple par exemple des Conclaves qui élisent les papes. La façon souple et fort adroite de régler les successions contribue beaucoup à la stabilité du régime. Et ce n'est pas de trop pour réguler les tensions politiques, toujours dans un esprit de conciliation. En effet, depuis l'existence du pays comme tel, deux forces contraires s'opposent. D'une part, les *wahdawis*, insistant sur la centralisation, et, d'autres part les fédéralistes, *ittihadis*[115]. Mais ces deux forces contraires, loin de devoir toujours être considérées comme pourraient bien réalité assurer un équilibre entre deux excès : celui de la désintégration d'une part, et celui d'une centralisation excessive de l'autre.

132. Ainsi, au terme de ce premier parcours, il est possible, peut-être, de dégager un premier constat. La concentration et la déconcentration ne constituent pas, en fait, une alternative, mais plutôt deux dynamiques complémentaires. L'important est alors de trouver un équilibre entre les deux, et le droit doit en quelque sorte s'évertuer de le promouvoir et de la sauvegarder.

[115] Cf. Malcolm PECK, « Formation and evolution of the Federation and its Institutions » , in Al IBRAHIM et Peter HELLYER, 2001, 145-160)

Section II : La concentration et la déconcentration des décisions à l'ère du numérique

133. En France, par exemple, la constitution de 1958 régit l'organisation politique des décisions propre à la cinquième République. Depuis, l'idée s'est imposée d'une décentralisation progressive et coordonnée, à savoir non d'une remise en cause de l'état unitaire comme tel au profit d'un état fédéral comme le sont les Emirats mais du moins d'un aménagement de ce dernier par le transfert des compétences administratives de l'Etat vers des entités à échelle plus réduite. La loi du 6 février 1992 relative à l'administration territoriale de la République, dite "loi ATR", marque un certain tournant au profit des collectivités territoriales et locales, comme les communes, les départements, les régions, les collectivités à statut particulier et les collectivités d'Outre-Mer.(communes, départements, régions, collectivités à statut particulier et collectivités d'outre-mer). Ainsi les collectivités territoriales se voient reconnaître une certaine autonomie d'action et de décision, en conformité avec la Charte européenne de l'autonomie locale de 1985, autonomie bien entendu circonscrite par les normes juridiques européennes et nationales et sous le contrôle de l'Etat. La décentralisation territoriale, qui est celle de conseils, régionaux, départements et municipaux, dont les membres sont issus des urnes, en vue de trancher des questions administratives, se prolonge, dans une même cohérence d'inspiration, en une décentralisation fonctionnelle ou technique bénéficiant aux établissements publics chargés de gérer un service public lui aussi, comme les université, les hôpitaux publics, les musées nationaux. Il faut reconnaître à la France le mérité d'avoir osé défier le poids de l'histoire de sa république pour s'engager dans une décentralisation effective un peu à rebours du fonctionnement centralisé qui a longtemps prédominé. L'objectif d'une telle politique de décentralisation, qui ne se réduit pas à la loi de 1992 mais a été relancée par le gouvernement Raffarin en 2003 avec l'Acte II de la décentralisation est double : d'une part, orienter les choix politiques de façon plus satisfaisante pour la population, plus au prise avec les problèmes concrets, et d'autre part, éviter la pesanteur d'un passage par le centre pour régler toute question périphérique. Mais s'y ajoute aussi, dans l'esprit de la République, une volonté d'éveiller chacun à sa conscience citoyenne.

134. La décentralisation se présente donc comme la traduction concrète et institutionnelle d'une exigence de déconcentration. La question qui se pose alors est de savoir, précisément, dans quelle mesure, une telle déconcentration est préférable à la concentration des pouvoirs de décisions, en sachant que fragmenter certaines décisions risque de faire un plusieurs vitesses.

Un exemple en cette rentrée 2017, la décision de la région Grand-Est de ne pas rembourser la tablette exigée dans le cadre scolaire, ainsi à charge des familles, contrairement à ce qui se passe dans les autres régions, ce qui peut engendrer insatisfaction et frustration. Si la France est devenue un pays centralisé, avec bien entendu un cortège de problèmes, c'est dans le prolongement de la nuit du 4 août 1789 pour mettre fin aux différents privilèges non seulement d'individus (personnes physiques) mais également de provinces, de principautés, de villes et de communautés d'habitants (personnes morales). En réalité, il semble, de façon plus complexe que ne peut le donner à penser un résumé simpliste, que l'organisation de nos institutions se soit fait dans le but d'éviter à la fois des inégalités entre régions et de remédier aux abus d'une centralisation qui étouffe la bonne marche des choses, trop procédurière, trop lente et souvent. C'est le 25 mars 1852, déjà, qu'est signé par le Président Louis-Napoléon Bonaparte (futur Napoléon III) un décret sur la centralisation administrative afin de trouver un équilibre, pourrait-on dire en termes actuels, entre concentration et déconcentration. Au demeurant, il est suggestif de relever la publication en 1865 à Nancy d'un opuscule sous le titre "un projet de décentralisation" qui reste dans l'histoire comme le célèbre "programme de Nancy". On y devine en filigrane la tension, propre à la France peut-être, entre Paris et la Province, laquelle Province regroupe à l'époque environ quatorze fois la population de la capitale. Deux grandes idées animent ce projet : d'une part, renforcer la commune et de l'autre émanciper le département. Mais la volonté de déconcentration se heurte non seulement à la résistance des volontés centralisatrices mais également à un processus qui n'est pas seulement administratif, mais tient à l'attractivité sociale, économique et culturelle de Paris aux dépends de tout le reste de la France, comme le souligne en 1947 l'ouvrage célèbre "Paris et le désert français"[116]. L'exode rural accéléré favorise une concentration de facto moins propice à une décentralisation administrative. Par la suite, des politiques d'aménagement du territoire sont menées, incitant par exemple des entreprises à s'installer ailleurs qu'à Paris. Le 22 octobre 1976, Olivier Guichard remet son rapport "Vivre ensemble" au Président Valéry Giscard d'Estaing formulant des propositions novatrices en matière de décentralisation qui seront reprises par la suite par Gaston Defferre, au début de la Président Mitterrand, en 1982. Cette histoire éclaire la situation actuelle de la France qui est singulière.

[116] Jean-François GRAVIER*, Paris et le désert français*, Paris, Le Portulan, 1947.

135. L'intérêt spécifique de la loi constitutionnelle du 28 mars 2003 est de donner une base solide à la déconcentration et à la décentralisation, autour des deux piliers que sont la subsidiarité et la proximité. Le pouvoir de décision administratif s'accompagne d'une reconnaissance de l'autonomie financière et d'une ouverture à la demande de participation populaire. La loi de réforme des collectivités territoriales du 16 décembre 2010 poursuit l'entreprise menée. Mais une attention particulière peut et doit peut-être être accordée à la loi du 27 janvier 2014 préconisant la "modernisation de l'action publique territoriale" et « l'affirmation des métropoles ». En effet, dans la perspective des idéaux républicains français, décentraliser ne veut pas dire simplement transférer de nouvelles compétences aux collectivités territoriales mais encore mener une réflexion de fond pour voir comment coordonner une politique d'ensemble en associant sans les court-circuiter les échelons locaux, pour plus de performance et de pertinence, en fonction des urgences qui se posent, à l'évidence différentes selon les lieux et les espaces géographiques. Dans le cadre spécifique de notre recherche, il ne nous appartient pas ici de relever en détails les dispositions par lesquelles la France met en œuvre une politique de déconcentration et de décentralisation [117] , sinon pour noter qu'un vrai souci inspire ces choix juridiques, celui d'une subsidiarité en acte. De toute manière, le progrès technologique bénéficie à chaque échelon dans la mesure où il compte sur des moyens incomparablement supérieurs à ceux du passé mais également dans la mesure où il peut ainsi être connecté à tous les autres, ce qui permet d'articuler l'autonomie et la concertation, en un temps très réduit. A cet égard, le bienfait du numérique relève de l'évidence. Sans dicter forcément un choix politique, il permet aux volontés de prendre corps. Tout projet peut d'une certaine façon s'appuyer sur lui. En tout cas, il constitue une opportunité de tenter de mettre en place un fonctionnement équilibré associant les avantages à la fois d'une proximité décentralisée et d'une harmonisation pour éviter l'éclatement.

136. Les Emirats bénéficient d'une constitution qui n'est devenue définitive, cependant, qu'en 1996. D'une part, dans la mesure où il s'agit d'un jeune pays mais également en raison de la volonté de privilégier le pragmatisme sur la lettre d'un texte même aussi autorisé. Le consensus, l'"ijma" traditionnelle, demeure une norme première et une pratique qui ne cesse de porter des fruits et

[117] Cf. Jacques BAGUENARD et Jean.-Marie. BECET, *La démocratie locale,* Paris, PUF, Que sais-je? 1995; Philippe BODINEAU et Michel VERPEAUX, *Histoire de la décentralisation*, Paris, PUF, Que sais-je?, 1993; Olivier DIEDERICHS et Ivan LUBEN*, La déconcentration*, Paris, PUF, Que sais-je?, 1995; Michel VERPEAUX et Christine RIMBAULT, *Les collectivités territoriales et la décentralisation*, 6e éd, Paris, La Documentation Française, 2011; compléter plus récent.

qui désamorce d'ailleurs de possibles conflits. Le local l'emporte par ailleurs sur le global, si l'on suit ce qu'énonce l'article 116 de la constitution où tout ce qui ne relève pas la compétence explicite de l'échelon fédéral relève de celui de chacun des émirats fédérés, quelquefois même pour certains accords internationaux, sous réserve d'en avertir le Conseil Suprême du pays, ou pour ce qui concerne l'adhésion à l'OPEP ou à *l'OPAEP*. Comme nous l'avons déjà établi précédemment cette valorisation très forte de l'échelon fédéré s'ancre autant dans une pratique séculaire qu'il ne fait écho à un souci de subsidiarité, conçu en des termes contemporains[118]. On ne le soulignera jamais assez, comme le rappelle justement Christopher Davidson, spécialiste reconnu de la question, que les Emirats s'appuient davantage sur leur héritage politico-culturel que sur leur constitution[119]. Cet ancrage dans la tradition est assez souple pour justifier et appuyer une ouverture aux valeurs occidentales (comme celles de la déconcentration et de la subsidiarité) par une sorte de va et vient entre le passé d'une part, et le présent, sinon le futur de l'autre. Ce socle, qui est un héritage de l'histoire, sur lequel s'appuient les Emirats pour bâtir l'avenir est peut-être, paradoxalement, l'explication d'une certaine décrispation qui lui permet d'envisager les défis avec pragmatisme, et volonté d'une modernisation des moyens et d'une vraie démocratisation[120]. On le comprend aisément, dans toute organisation fédérale, la répartition des fonctions est complexe, controversée et parfois évolutive. A l'échelon fédéral, se trouvent concentrées les attributions régaliennes, comme les Affaires étrangères, la monnaie, la défense, les grandes questions migratoires. Comme il se doit dans un état qui se veut fédéral, l'article 116 énonce le principe suivant : « toutes les affaires qui ne sont pas expressément stipulées comme étant du ressort fédéral appartiennent en propre au domaine de l'émirat ». Le plus intéressant, néanmoins, est sans doute le fait que des accords internationaux peuvent être conclus y compris par chacun des Emirats, pour peu qu'ils concernent des problèmes spécifiquement locaux comme l'énonce l'article 123. Il faut également que le Conseil suprême ait été averti au préalable. En pleine cohérence avec cette orientation foncièrement fédérale, chaque émirat peut prendre l'initiative d'adhérer à l'Organisation des pays exportateurs de pétrole (OPEP) ou même à l'organisation des pays arabes exportateurs de pétrole » (OPAEP),

[118] Cf. Malcolm PECK, "Formation and Evolution of the Federation and its Institutions" in Ibrahim ABED et Peter HELLYER (dir.*), United Arab Emirates. A New Perspective*, Londres, Trident Press, 145-160.
[119] Christopher DAVIDSON, "The Emirates of Abu Dhabi and Dubaï. Contrasty roles in the international system" in *Asian Affairs*, 38, 1, mars 2007, 33-48*; The United Arab Emirates. A Study in Survival*, Boulder, Lynne Rieder Press, 2005.
[120] Cf. Ibrahim ABED, "The historical background and constitutional basis to the federation" in Ibrahim ABED et Peter HELLYER*, op. cit,* 162-176.

même si cette possibilité est en réalité assez théorique dans la mesure où l'exploitation pétrolière se fait essentiellement à Abu Dhabi.

137. La volonté de démocratisation sur fond de déconcentration ne cesse cependant de se renforcer. En 2005, Khalifa Ben Zayed Al Nahyane précise que désormais sur les quarante membres du Conseil national fédéral la moitié serait élue, tandis que l'autre resterait désignée. Les différents candidats sont des différents émirats pour que tous soient ici représentés. On peut noter que le cheikh a favorisé les candidatures féminines devant ainsi l'évolution de la société du pays, encore rétive au départ à accepter l'égalité femme / homme en politique de sorte qu'une seule femme a été élue lors des élections de 2006, alors que près d'un candidat sur cinq était une candidate. En revanche, sur les vingt membres désignés huit sont des femmes. Quelques années plus tard, dans une interview remarquée, Abdul Aziz Al Ghurair, président du Conseil national fédéral parle de la démocratisation comme un processus graduel qui est bel et bien engagé[121]. Le concept central de la politique mené est celui de *shura,* à savoir de consultation. Les élections de 2011 voient une plus large implication des femmes. Il faut bien dire que les autorités fédérales poussent à la roue et veulent favoriser un élargissement du corps électoral. A nouveau, une seule femme est élue, Shaika Eisa Ganem Al Arri, ce qui veut dire que les évolutions sont lentes. Le souci des cheikhs est de promouvoir la tolérance, notamment entre sensibilités religieuses et tribus. Les enjeux des élections ne sont pas idéologiques, car les candidats ne représentent pas différents partis qui auraient chacun une visée très définie et exclusive. Il s'agit plutôt de distinguer les compétences des différents candidats, d'où aussi l'utilisation des réseaux sociaux pour faire ressortir les traits saillants des personnalités.

138. Plutôt qu'une décentralisation territoriale, c'est une mutation dans la continuité de l'identité du pays que les Emirats doivent affronter. Le fait qu'en raison du nombre très important de travailleurs étrangers les Emiriens se sentent parfois minoritaires – et le sont numériquement puisqu'en 2010 sur le territoire des Emirats vivent plus de 7 millions d'étrangers et même pas un million de personnes originaires du pays - implique bien une recherche d'équilibre entre l'ouverture mondiale, garantie au niveau fédéral, et la préservation de l'identité locale. Par ailleurs, si la plupart des pays connaissent une concentration autour de la capitale, comme c'est le cas en particulier de la France, où Paris occupe une place unique dans le pays, en raison d'un

[121] Cf. « Democratisation is a Gradual Process » in *Gulf New*s, 25 décembre 2008.

ancien modèle politique très centralisé, les Emirats sont très différents par leur étendue, leur population, leur évolution économique, le niveau de leur industrialisation. En lien direct avec la grande disparité entre les Emirats se trouve une tendance actuellement très forte de renvoi des Emiriens aux marges du pays, alors que dans les zones plus riches et plus développées la proportion des étrangers est beaucoup plus forte. Cela s'explique bien entendu par le besoin d'une main d'œuvre étrangère forcément plus fort là où il y a du travail à faire que là où il n'y en a pas. En tout cas, la très forte croissance a favorisé un certain clivage entre les espaces géographiques, et parfois même les quartiers d'une grande ville comme Dubaï. Les Emiriens se sentent d'ailleurs comme pris en étau entre leur ouverture internationale et leur ancrage local, l'échelon national du pays se trouvant en quelque sorte à l'interface, ce que lui donne à la fois une importance stratégique mais risque aussi de faire se dissoudre sa consistance propre. De sorte que, quelquefois, la question peut légitimement se poser de l'identité commune possible entre d'une part l'affirmation traditionnelle d'un ancrage dans un lieu, et l'ouverture internationale, rendue évidente et urgente pour des raisons économiques et commerciales. Or, les politiques qui ont une unité politique tardive (XIXe siècle) comme l'Italie ou l'Allemagne bénéficient du ciment de la langue commune, même s'il y a des variations dialectales quelquefois significatives. En revanche, dans les Emirats on parle plusieurs langues comme le farsi, le hindi et l'ourdou. Certes, l'anglais devient une sorte de langue commune, mais c'est justement la langue internationale, celle du commerce, et la langue vraiment nationale, facteur de civilisation. Loin de véritablement unifier, l'anglais semble au contraire accroître le clivage interne entre des classes, favorisée et défavorisée (Sally FINDLOW[122]. Qui plus est, il y a une concurrence désormais entre l'anglais et l'arabe, chacune des langues incarnant en quelque sorte l'un des aspects plus ou moins en contradiction. D'une part, la modernisation sur fond d'internationalisation ; d'autre part, la défense de la trahison et de la cohésion du pays[123]. Une certaine réaction s'est manifestée ces dernières années, pour réagir contre l'anglicisation forcenée, incluant l'obligation de préparer tous les documents officiels dans la langue traditionnelle, l'arabe. Mais dans le privé, il en va très différemment. L'arabe serait un obstacle aux échanges avec les entreprises internationales. Par pragmatisme, l'anglicisation est encouragée. C'est pourquoi on peut dire aujourd'hui que l'anglais s'impose véritablement

[122] « Higher education and linguistic dualism in the Arab Gulf British » *in Journal of Sociology of Education*, 27, 1, 19-36, 2006)

[123] Matthew CLARKE, « Language policy and language teacher education in the United Arab Emirates » in *Quarterly,* 41, 3, 583-591, 2007.

comme la langue des Emirats, le bilinguisme n'en étant plus véritablement un[124]. Pour compenser cette éclipse du sens d'identité, les autorités misent sur la valorisation du patrimoine archéologique ou architectural[125]. Dans l'émirat de Charjah, en particulier, le projecteur est placé sur les musées. Cette valorisation du patrimoine, dans le souci d'un renforcement du sens de l'identité des Emiriens, s'accompagne également du développement de l'attraction touristique[126]. A nouveau, il y a un équilibre, un balancement, un mouvement de systole et de diastole entre deux pôles opposés, comme entre centralisation et déconcentration dans les pays occidentaux. Il va de soi que le patrimoine n'est pas seulement bâti mais inclut également le costume, les coutumes, y compris d'anciens divertissements comme les courses de chameaux. La réaffirmation d'usages parfois constitue bien une sorte de résistance au nivellement induit par l'internationalisation que favorise d'ailleurs la révolution numérique, mais il ne faudrait lui donner une finalité uniquement négative. Sans aucun doute, l'adhésion à des valeurs et à des pratiques commune vise-t-elle d'abord à sceller des liens entre Emiriens, et à trouver des références communes aux sept entités fédérées[127].

139. Le sentiment d'une identité malaisée à identifier et aujourd'hui très fragilisée conduit à une politique d'émiratisation des Emirats, à savoir de renforcement de l'engagement de la population locale à tous niveaux et de l'affirmation plus forte d'une identité commune. Dans d'autres pays, qui pour des raisons économiques, accueillent beaucoup d'étrangers, un tel processus s'est déjà vérifié de par le passé, comme par exemple au Koweït où a eu lieu une « koweïtisation »[128]. L'objectif est de pousser les citoyens du pays à y occuper les postes de la vie active, pour ne pas être supplantés par les étrangers dans le pays. Le même processus se vérifie aussi à Oman quelques années plus tard. Dans les années 1990, on assiste à un phénomène de « saoudisassions ». Puis, c'est le cas de Bahreïn, dans un contexte qui ressemble beaucoup à celui des Emirats. Les entreprises doivent augmenter leur quota de nationaux. Or,

[124] Kay GALLAGHER, « Bilingual Education in the UAE. Factors, variables and critical questions » in *Education, Business and Society. Contemporary Middle Eastern Issues*, 4, 1, 62-79, 201.
[125] Fred LAWSON et Hasan M. AL NABOODAH, « Heritage and cultural Nationalism in the United Arab Emirates » in Alanoud ALSHAREK et Robert SPRINGBORG (dir.*), Popular Culture and Political Identity in the Arab Gulf States*, Londres, Saqi, 15-30, 2008.
[126] Sulayman KHALAF, « Globalization and heritage revival in the Gulf. An anthropological look at Dubai Heritage Village » in *Journal of Social Affairs*, 19, 75, 277-306, 2002.
[127] Sulayman KHALAF, « National dress and the construction of Emirati cultural identity » in *Journal of Human Sciences*, Bahrain University, 11, 230-267, 2005.
[128] Amr EL-SHALAKANI, Amal EL-SABAH, Marwan ISKANDER, « An optimized model for substitution of expatriate workforce in a Gulf-Council country : the Kuwaiti Case », in *International Migration*, 34, 2, 273-295, 1996.

aux Emirats beaucoup de jeunes du pays n'ont ni travail, ni formation[129]. Il est vrai d'une certaine façon qu'aux Emirats les autorités se livrent à une répartition des secteurs d'activité pour déterminer ceux où il est préférable que soient embauchés des locaux[130]. Comme cela est très compréhensible pour un pays, les Emirats entendent accroître leur présence dans des postes d'autorité et de gouvernance, plus valorisant pour leurs citoyens[131]. De façon assez récente, le plus apporté par les femmes est bien mis en valeur au sein des Emirats, y compris dans le cadre professionnel[132].

140. Le ministère du travail et des affaires sociales est à l'origine le maître d'œuvre de l'émiratisation. Une agence a été mise en place, *Tanmia*, pour maximaliser les initiatives. En matière de droit du travail, la législation accorde aux Emiriens des conditions avantageuses. Du point de vue du maillage territorial du pays, on assiste à des déménagements, par exemple à cause de l'augmentation des loyers. Mais le plus significatif demeure certainement la façon dont est gérée la concurrence entre Abu Dhabi et Dubaï, en vue d'une complémentarité et d'un équilibre entre les deux[133]. Les deux émirats ont leur spécificité propre dans le développement économique et les deux cités-phares peuvent ainsi se compléter. Après une phase montante pour Dubaï, aussi pour des raisons touristiques, c'est aujourd'hui Abu Dhabi qui semble renforcer sa domination qui redevient la « locomotive de la fédération »[134]. Le point qu'il semble important de souligner ici est la volonté d'équilibre qui caractérise la politique des Emirats entre ce processus d'émiratisation d'une part et d'autre part une véritable volonté d'ouverture dans la claire prise de conscience du bienfait pour le pays des échanges internationaux. Cet équilibre, qui est parfois un balancement selon les urgences de l'heure, n'est pas sans faire penser à celui qui peut être recherché dans une problématique à la fois voisine et différente entre la concentration et la décentralisation. Le numérique semble pouvoir réguler des flux, ajuster des stratégies, par exemple fixer un taux voulu de locaux dans telle responsabilité et surtout vérifier qu'il est effectivement respecté. En tout cas, au-delà des choix qui relèvent d'une stratégie

[129] Sultan AL AZRI, *Unemployed Youth in the UAE. Personal Perceptions*, lnc, Diane Publishing, 2010.
[130] Mervin J. MORRIS, « Organisation, social change and the United Arab Emirates » in Social Change in the 21st Century Conference, 28 octobre, Centre for Social Change Research, Queensland University of Technology, 2005)
[131] Paul A. ELSNER et James HORTON, « Higher Colleges of technology United Arab Emirates » in Paul A. ELSNER, George R. BOGGS et Judith T. IRWIN (dir.), *Global Development of Community Colleges*, Technical College and Further Education Programs, Washington, 149-160, 2008.
[132] Vania CARVALHO PINTO, *Nation-Building State and the Genderframing of Women's Rights in the United Arab Emirates (1971-2009),* Reading, Ithaca Press, 2012.
[133] Cf. l'étude la plus importante sur le sujet : Christopher DAVIDSON, « The Emirates of Abu Dhabi and Dubai. Contrasting roles in the international system » in Aslan Affairs, 38, 1, mars, 33-48, 2007.
[134] William GUERAICHE, 2007, 312.

politique qu'il n'est pas directement de notre ressort d'analyser ainsi, il ne fait guère de doute que le numérique, par le gain en efficacité qui est le sien, peut largement contribuer à une politique d'équilibre entre des tendances opposées mais en réalité complémentaires et à un ajustement constant entre des exigences opposées.

TITRE II : L'EFFICACITE D'UN FONCTIONNEMENT PLUS DEMOCRATIQUE

141. Dans le monde qui est le nôtre, il semble que le critère essentiel ne soit plus tant la valeur objective des choses que l'efficacité, le rendement. La philosophie globale qui nous entoure est fortement pragmatique[135]. Cela paraît singulièrement vrai dans la conception de la démocratie comme devant contribuer à un fonctionnement social plus efficace. Dans cette perspective, elle n'est pas d'abord un mode de gouvernement découlant de la reconnaissance théorique d'une souveraineté, mais une façon de gérer les conflits inévitables entre les valeurs en présence, et souvent en tension, et les différents intérêts. En définitive, elle implique la participation de tout être humain à la mise en forme d'un édifice de valeurs permettant le développement de la personnalité de chacun et de tous aussi. Cette orientation politique et philosophique est développé en particulier par le penseur et psychologue américain John Dewey mais imprègne notre culture occidentale au moins après la Seconde Guerre Mondiale[136]. Ainsi la notion même de démocratie va beaucoup plus loin qu'un concept de droit constitutionnel : elle désigne, dans une perspective dynamique et pragmatique, une intention éthique fondamentale. Elle est donc mesurée non pas tellement par sa conformité avec des principes juridiques abstraits donnés dès le départ mais par la réussite ou non des objectifs devant répondre à des valeurs à réaliser concrètement, aussi individuellement que collectivement. Cela conduit à une vision de la démocratie, non en amont, mais en aval, en fonction de ce qu'elle permet ou non de réaliser. En d'autres termes, le droit ne devra pas définir un contrat à respecter, indépendamment de sa réussite, et loin de toute culture du résultat, au contraire se forger dans le souci constant de bonnes conséquences.

142. D'une certaine façon, sans perdre toutefois leur évidente nécessité, les grandes institutions deviennent plus contingentes, plus flexibles, contestables même, toujours en regard du résultat. C'est cette culture du résultat qui bouscule sans doute une approche plus statique du droit. C'est la projection vers le futur qui doit orienter ses choix, bien entendu plus incertain que sous la forme d'une sorte de déduction de principes très définis. Or, cette nouvelle perspective s'harmonise singulièrement bien avec l'univers des nouvelles technologies où domine le critère d'efficacité et de rentabilité, mais pas forcément en termes uniquement pécuniers, mais aussi de gratifications subjectives – on pense aujourd'hui à la perspective du développement

[135] Jean-Pierre COMETTI, *Qu'est-ce que le pragmatisme*, Paris, Gallimard, 2010.
[136] Gérard DELEDALLE*, John Dewey*, Paris, PUF, 1995.

personnel - , se révèle aussi important. Les résultats attendus nous semblent se trouver aussi bien *ad intra* et *ad extra* : à savoir, dans le fonctionnement interne et dans les relations avec les extérieurs. Il va de soi qu'un certain lien associe ces deux dimensions, mais elles doivent néanmoins être distinguées, au moins dans une perspective de méthode.

Chapitre I. Le numérique pour des politiques publiques plus efficaces.

143. Il va de soi que des politiques publiques visent l'efficacité mais précisément, et de plus en plus, au sens où le pragmatisme imprègne leurs visées, mais aussi l'opinion en général, dont elles doivent tenir compte, pour éviter des sanctions à plus ou moins long terme, à commencer par celle des urnes, ou dans d'autres cas d'une mise en cause violente du pouvoir en place pouvant aller jusqu'à un renversement du régime, comme cela a été le cas, entre autres, en Egypte. C'est vrai, il importe toujours de garder à l'esprit combien la notion d'efficacité est vaste et à certains égards un peu floue. Si l'on reprend des termes philosophiques, elle s'assimile à ce que Kant appelle un « jugement réfléchissant »[137] à savoir une évaluation qui ne bénéficie pas d'un critère clairement défini au départ et pourtant renvoie bien à une certaine objectivité, et ne se réduit pas à un pur arbitraire individuel et collectif, les uns trouvant efficace ce que d'autres ne trouveraient pas efficace, et les uns et les autres ayant le droit de penser ce qu'ils veulent, sans que n'intervienne l'idée d'une vérité objective. A l'évidence, la question de l'efficacité ou non d'une mesure ou d'une politique, comme d'ailleurs de n'importe quel moyen, y compris le plus concret comme la scie en menuiserie ou telle machine plus perfectionnée, semble devoir pouvoir être tranchée de façon objective. Elle renvoie donc à une réelle objectivité : celle de la conformité d'un effet produit par rapport à une fin. A plus large échelle, du résultat par rapport à une attente, à un espoir, à un horizon entraperçu parfois plus que clairement défini d'amélioration globale. Dans un certain nombre de cas, l'efficacité parait très mesurable. Ainsi, un rasoir sera jugé efficace s'il rase bien et de près. Mais le but recherché d'une politique est plus global et plus complexe, renvoyant à une certaine vision de ce qu'est une société bonne, laquelle n'est peut pas partagée par tous mais conçue de façon différente selon la vision des choses et de la vie propre à chacun. D'emblée nous pouvoir voir ainsi combien la tâche du juriste est alors rendue plus complexe, plus délicate, et plus incertaine, en fonction des priorités choisies. Nous sommes loin d'une sorte de déduction mathématique qui s'imposerait. De plus, le conflit entre les valeurs, sorte de guerre des dieux[138] rend difficile le consensus sur un idéal à viser. Faut-il par exemple promouvoir des valeurs d'intégrité, au sens le plus rigoureux, et

[137] Emmanuel KANT, Kant, Critique de la faculté de juger, présentation et traduction par Alain Renaut, Paris, Aubier 1995 ; Gérard LEBRUN, *Kant sans kantisme*, Fayard, 2009 (posthume), « III- L'Unité retrouvée de la troisième Critique », p. 167-258 ; Alexis PHILONENKO, *L'œuvre de Kant*, Vrin, 1972, vol. II. La singularité du jugement réfléchissant et son implication décisive pour toute la pensée de Kant a été mise en valeur, de façon très claire, et dans la veine de Philonenko, par Luc FERRY, *Kant : une lecture des trois « critiques »*, Paris, Grasset, 2006.

[138] Au sens de Max WEBER, à savoir d'affrontements entre diverses conceptions du bien de la société à partir d'accents différents sur telle valeur ou telle autre, ce qui rend improbables et partisans les choix politiques : cf. Sylvie MESURE et Alain RENAUT, *La guerre des dieux. Essai sur la querelle des valeurs*, Paris, Grasset, 1996.

pour les garantir imposer une sorte de transparence, par exemple en faisant disparaître les liquidités au profit d'échanges dématérialisés tous vérifiables ? Mais alors qu'en va-t-il de la liberté et aussi du droit à la protection de la vie privée, car chacun n'a peut-être pas envie de faire savoir quels sont ses goûts et ses préférences en matière de dépense ? Faut-il placer l'accent sur l'égalité concrète au détriment peut-être d'une équité plus fondamentale et de la liberté ? Par exemple en dressant des cartes scolaires obligatoires, soigneusement respectées ou dans l'attribution de peines qui éluderaient le facteur humain et les degrés divers de responsabilité subjective à évaluer comme de ressenti des peines infligées ? Convient-il de renforcer la protection individuelle, par exemple en versant des assurances sociales plus consistantes, ou en revanche de responsabiliser les individus, les forçant par exemple à éviter des dépenses de santé inutile ou à rechercher réellement un nouvel emploi sans tarder ? Nous sommes là en présence de choix de société qui sauf positions extrêmes connaissent toute une gamme d'options possibles et démocratiquement acceptables pour les décliner. Cette complexité rend plus improbable la notion d'efficacité car précisément l'idéal visé, au moins dans le concret de l'histoire, n'est pas le même pour tous. Du reste, le numérique ne change pas fondamentalement cette donnée car si elle maximalise l'efficacité comme telle elle ne clarifie pas forcément les buts visés. Au contraire, il pourrait plutôt rendre plus opaque une réflexion de départ, car il nous grise et nous fait parfois oublier la délibération initiale de départ pour nous laisser entraîner vers ce que suscite de façon presque automatique la nouvelle technologie à l'œuvre, comme l'illustre la caricature du *geek*, qui est en quelque sorte l'esclave des nouvelles technologies dont il devient dépendant, et qui le conduisent où elles veulent. Une réflexion ne cesse de se développer sur d'éventuelles conséquences négatives induites par le numérique, et pas seulement de la part de ceux qui seraient rétifs à toute évolution, ou désemparés face à des techniques qui leur font peur, et qui s'imposent à eux, ne serait-ce que pour déclarer ou payer leurs impôts en ligne. Des sociologues pointent du doigt aussi bien la menace de lancer des réalisations qui nous échappent que d'aggraver ainsi la fracture sociale, entre ceux qui sauront se mouvoir dans ce nouvel univers, ou éventuellement s'appuyer sur la compétence technique d'autres, et ceux qui resteront au bord du chemin. Ils ne doutent pas de l'efficacité intrinsèque et toujours de plus en plus évidente du numérique, mais se demande où cela va nous conduire[139]. La notion même d'efficacité des politiques publiques semble ainsi discutable, et ce d'autant plus que certains pourraient même mettre en cause l'idée de son bien-

[139] Françoise THIBAULT et Clément MABI*, Le politique face au numérique : une fascination à hauts risques Politics and the challenge of the digital era: a high-risk fascination*, http://journals.openedition.org/socio/1344

fondé. Est-il vraiment souhaitable que les politiques publiques soient efficaces, ou cette qualité ne relève-t-elle pas plutôt de l'initiative privée ? Les politiques publiques ne seraient-elles pas plutôt destinées à créer un cadre dans lequel l'efficacité des initiatives privées pourrait fleurir et ne pas être compromise ou freinée par des intrusions malheureuses, des réglementations tatillonnes ou un contrôle sourcilleux qui paralyserait tout ? Selon un mot célèbre, il ne s'agirait pas tant de régler les problèmes de l'Etat, mais d'éviter que l'Etat lui-même ne soit un problème. Selon un positionnement libéral[140], en fait, le rôle des politiques publiques doit être limité, plus « négatif » que « positif », de protection de l'intégrité et de la liberté des individus, plus que relance de l'économie ou de combat des inégalités. Toutefois, même en acceptant cette vision très libérale des choses, qui rétrécit le rôle dévolu aux politiques publiques, il n'en reste pas moins que dans les secteurs où elles s'imposent, comme la police ou la justice, les politiques publiques sont appréciées positivement si elles sont efficaces, et critiquées si elles ne le sont pas.

144. Ainsi donc, l'efficacité, non réduite à un aspect de pur profit économique et financier, mais orientée vers des valeurs, trouve-t-elle sa place dans une société démocratique soucieuse d'un bon fonctionnement, justement pour correspondre de façon de plus en plus adéquate à ce qu'elle veut être, en l'occurrence justement démocratique. Bien entendu, les contours précis de cette notion sont flexibles et même flous de sorte que le juriste peine à voir comment l'inscrire convenablement dans un édifice juridique. Pour autant, l'efficacité demeure incontournable. D'une certaine, on en perçoit plus la valeur et l'importance lorsqu'elle fait défaut. Elle pourrait d'ailleurs être surtout définie négativement, à partir de disfonctionnements évités, ou de lenteurs conjurées. L'efficacité se présenterait alors surtout comme la facilité d'éviter des empêchements, des obstacles et des freins, ce qui permet une approche juridique plus consensuelle que celle qui tente d'y voir une maximalisation des moyens en vue de fins que tout le monde ne définit pas de la même manière. Dans son livre célèbre de 1971, *Théorie de la justice*[141], John Rawls avait noté qu'il n'est pas nécessaire d'être d'accord au fond sur ce qu'est le bien en soi, sur sa nature et ses principes, pour formuler une morale qui combatte ce qui d'évidence sera un disfonctionnement éthique, en l'occurrence de graves inégalités. De même,

[140] Présentation claire et engagée d'une telle vision : Raymond BOUDON, *Pourquoi les intellectuels n'aiment pas le libéralisme*, Paris, Odile Jacob, 2004.
[141] John RAWLS*, Théorie de la justice*, tr. Fr. Catherine AUDARD, Paris, Seuil, 1987 [1971]. Même si cette position minimaliste est encore trouvée trop limitative pour la liberté par certains autres philosophes comme Robert NOZICK, Anarchie, Etat et utopie, tr. Fr., Paris, PUF, 1974.

mutatis mutandis, il n'est pas nécessaire de définir par le menu un Etat bon pour combattre ce qui l'empêche de le devenir. En ce sens, il y a une efficacité en quelque sorte « négative », au sens où elle empêche des disfonctionnements, plus facile à énoncer et moins susceptible de divergences. Plus problématique sans doute demeure l'efficacité en quelque sorte « positive » des effets induits que d'aucuns jugeront en fait indésirables, comme par exemple la restriction possible de la vie privée en raison d'un souci de transparence. En tout cas, l'efficacité procurée ou renforcée par le numérique s'impose d'abord comme un fait, quelle que soit évaluation, favorable ou défavorable, que l'on puisse en faire dans le cadre d'un projet de société.

Section I : Les technologies nouvelles, facteur d'une efficacité renforcée

145. Il nous faut ainsi partir d'un inventaire de l'existant pour reconnaître, en amont du jugement de valeur porté, les conséquences déjà induites et aussi en quelque sorte probables, des nouvelles technologies dans le sens d'un meilleur fonctionnement. D'une part, le numérique évite un surcroit de travail, du temps perdu, de la confusion inévitable. Il favorise ainsi une simplicité que pour le coup personne ne saurait contester ainsi exprimée au Moyen Age par cette devise de Guillaume d'Ockham (XIVe siècle) : *« entia non sunt multiplancada sine necessitate* » (il ne faut pas multiplier les choses superflues). D'autre part, il contribue en positif à des résultats jusqu'alors non espérés, ou en tout cas non obtenus.

a) Des disfonctionnements évités

146. Si l'existence de la démocratie comme telle semble remonter aux Chinois d'il y a plusieurs siècles, il ne fait guère de doute qu'elle s'est développée de façon exponentielle au fil des âges, et surtout ces dernières décennies. Du reste, nous assistons là à une sorte d'effet pervers des progrès techniques qui loin de contribuer à la simplification peuvent au contraire ajouter des complications, au moins un certain temps. En France[142], par exemple, l'administration qui doit beaucoup à un Colbert, parmi d'autres, à l'époque de Louis XIV constitue non seulement une force mais un handicap par sa lourdeur, son inertie, que les politiques tentent souvent vainement de réformer. Les sociologues depuis Max Weber[143] jusqu'à Michel Crozier[144], en passant par le plus discuté Octave Gélinier[145], qui veut lui substituer un management plus efficace, tentent d'en analyser les ressorts et les pesanteurs, d'ailleurs également subies et déplorées au quotidien par chacun d'entre nous. L'administration peut se définir en droit comme l'ensemble de ce qui touche à l'organisation et à l'action dans la sphère publique, étant évident qu'il existe aussi des formes équivalentes, mais souvent moins lourdes, dans le secteur privé. La norme européenne de comptabilité nationale définit ainsi l'administration publique[146] : « l'ensemble des unités institutionnelles dont la fonction principale est de produire des services non marchands ou

[142] Guy THUILLIER et Jean TULARD, *Histoire de l'administration française*, Paris, QSJ, PUF, 1994 ; Yves THOMAS, *Histoire de l'administration*, Paris, La Découverte, 1995.
[143] Hubert TREIBER, « Etat moderne et bureaucratie moderne chez Max Weber » in Andreas ANTER et Stefan BREUER (dir.), *Max Webers Staatssoziologie. Positionen und Perspektiven*, Baden-Baden, Nomos Verlag, 2007, 121-155.
[144] Michel CROZIER, *Le phénomène bureaucratique*, Paris, Seuil, 1963.
[145] Octave GELINIER, *Fonctions et tâches de direction générale*, Paris, Éditions Hommes et Techniques, 1963.
[146] *Système Européen de Comptabilité*, 1995.

d'effectuer des opérations de redistribution du revenu et des richesses nationales. Elles tirent la majeure partie de leurs ressources de contributions obligatoires ». De façon plus spécifique, on peut dire que l'administration publique se compose de l'administration centrale, territoriale ou de sécurité sociale. Dans son traité qui fait date de 1812, *De l'importance et de la nécessité d'un code administratif*[147], Charles-Jean Baptiste Bonnin tente précisément de mettre en valeur le critère d'efficacité comme le plus adapté à une bonne administration. En France a été créée dans ce but en 1945 par Michel Debré, l'ENA (Ecole Nationale d'Administration), aujourd'hui critiquée[148], mais toujours prestigieuse[149], d'autant plus qu'un grand nombre des dirigeants de notre pays, et des grands chefs d'entreprise, en sont issus. En raison précisément de sa nature et de ses objectifs, dans le souci d'une efficacité qui suppose l'adaptation à un contexte de plus en plus mouvant, l'administration doit sans cesse être modernisée. Cette exigence lui est en quelque sorte connaturelle pour correspondre à sa mission[150]. Dans cette même perspective d'efficacité et d'économie de moyens et d'argent, le nouveau Premier Ministre Edouard Philippe a défini en 2017 l'initiative « Action publique 2022 »[151] dans laquelle il envisage d'importantes réformes, sans négliger le travail sur la transformation numérique qui est un point de priorité.

147. Dans de très nombreux secteurs, d'ores et déjà, le numérique permet d'éviter les lenteurs et les frais, mais aussi l'aléatoire de la voie postale d'autrefois. L'information parvient aux destinataires en temps réel et peut-être traitée immédiatement. Les nouveaux procédés de classement permettent au demeurant d'éviter des confusions et des recherches inutiles. En ce qui concerne la transmission des connaissances, elle devient plus rapide, moins onéreuse et davantage interactive depuis la révolution numérique.

b) Des opportunités indéniables.

[147] Charles-Jean Baptiste BONNIN, *De l'importance et de la nécessité d'un code administratif*, Paris, Gamery, 1812. Cf. Pierre ESCOUBE, « Charles-Jean Bonnin, précurseur de la science administrative », *La Revue administrative*, 61, janvier-février 1958, pdf en ligne.
[148] Jacques MANDRIN, *L'Énarchie ou Les Mandarins de la société bourgeoise,* Paris, Éditions de la Table ronde, 1967 (en fait il s'agit de Jean-Pierre Chevènement, de Didier Motchane et d'Alain Gomez) ; Pierre-Henri d'ARGENSON, *Réformer l'ENA, réformer l'élite - pour une véritable école des meilleurs*, Paris, L'Harmattan, coll. « Questions contemporaines », 2008.
[149] Odon VALLET*, L'école*, Paris, Albin Michel, 1991.
[150] Manuel DELAMARRE, Eric GRISTI, *Comprendre l'administration - Organisation, fonctionnement, modernisation,* Paris, DF, 2004.
[151] http://www.gouvernement.fr/partage/9603-lancement-d-action-publique-2022

148. Sans aucun doute, outre le fait de surmonter des dysfonctionnements, le numérique offre des opportunités considérables dont il est impossible de dresser une liste exhaustive mais qui s'impose d'ores et déjà par son ampleur. Bien entendu, le numérique favorise une plus grande qualité des services, conséquence directe de la lutte contre les dysfonctionnements. D'un autre côté, elle permet à tous de bénéficier d'un cadre de travail innovant et modernisé. En matière de politique éducative, la diffusion des nouvelles technologies favorise l'apprentissage, même si le coût impliqué, au moins au départ, retarde la mise en place d'une infrastructure souhaitable. Désormais, plus de la moitié des collèges en France, par exemple, sont bien équipés. Au niveau de l'enseignement supérieur et de la recherche, l'articulation entre les méthodes classiques et les nouvelles technologies s'avère incontournable et fructueux. Les politiques publiques doivent créer une émulation[152]. Parmi les investissements d'avenir qui portent déjà du fruit il faut signaler les programmes liés aux Réseaux d'Initiative Publique (RIP) de haut et de très haut débit, l'internet des objets, les plateformes en ligne, l'identité numérique, la captation facilitée des informations mais également l'exploitation des données, pour lutter contre le banditisme ou l'évasion fiscale. Les développements de la modélisation favorisent une prospective plus fiable et donc plus utile, et pas seulement pour la météo. Une marge d'incertitude existe toujours mais il est désormais possible de l'évaluer.

149. Plusieurs vastes domaines de politiques publiques peuvent certainement être révolutionnés par le numérique comme ceux de l'accessibilité aux handicapés, en particulier grâce à une information ajustée et cohérente, encourageante aussi, ceux de la lutte contre la pauvreté, ceux de l'emploi ou ceux du développement durable. Les enjeux y sont considérables. Il s'agit de mettre concrètement en place des stratégies souhaitées. Dans de nombreux pays comme la France, une politique publique doit être mise en place pour la reconquête de l'industrie.

150. Il est intéressant à cet égard, d'évoquer l'histoire de l'avancée du numérique en France, qui peut inspirer l'avancée future des Emirats, qu'elle précède chronologiquement. La communication devient une dimension de plus en plus importante depuis plusieurs décennies, et ce dès les

[152] David ENCAOUA, « Interactions scirence-technologie : quelles politiques publiques ? », *https://www.cairn.info/revue-francaise-d-economie-2010-4-page-75.htm*.

années cinquante avec la télévision. En 1978, le rapport Nora-Minc[153] devance la future révolution informatique jugée encore bien insolite, alors, par une majorité de la population. Après une période un peu floue, où le scepticisme voisine parfois les rêves les plus délirants, l'informatique finit par s'imposer à vitesse croissante, fragilisant les anciennes institutions et les structures traditionnelles de pouvoir. Le processus de mutation coïncide avec le traité de Maastricht de 1992 et le remplacement partiel des souverainetés nationales par un pouvoir technocratique à l'échelle d'une partie du continent, tandis que se construisent les autoroutes de l'information. C'est en 1994 qu'internet arrive en France, et qu'une page nouvelle s'ouvre, autorisant des projets jusqu'alors improbables. Le Premier Ministre Lionel Jospin propose en 1997 un « programme d'action gouvernementale pour l'entrée de la France dans la société de l'information » (PAGSI)[154], insistant sur les secteurs de la culture et de l'éducation. Au début, les Français traînent un peu les pieds (en 2002, le taux de connexion à Internet dans l'hexagone est inférieur à celui de l'ensemble de l'Europe) mais les gouvernements entendent permettre au plus grand nombre possible de Français de bénéficier du haut débit. La problématique se déplace de la volonté de diffuser les nouvelles technologies à celle de les contrôler et de réprimer, graduellement il est vrai, les différents abus, comme le téléchargement illégal. En témoigne, par exemple, la création de la haute autorité de protection des droits sur Internet[155]. En 2011, est établi le Conseil National du Numérique (CNN)[156] pour aborder les questions nouvelles. L'accent est placé sur la sécurité renforcée que permet le numérique, par exemple dans les domaines de la pédopornographie[157], de la prostitution, du proxénétisme et plus encore du terrorisme, devenu une question prioritaire depuis l'attaque des Twin Towers new-yorkaises en 2001.

151. En 2016, le Premier Ministre Manuel Valls propose une loi pour une république numérique[158]. L'axe reste placé sur la sécurité, l'urgence faisant loi, comme l'attestent la loi de programmation

[153] *http://www.ladocumentationfrancaise.fr/rapports-publics/154000252/index.shtml.* Sur ce rapport : cf. Andrée WALLISER, « Le rapport Nora-Minc. Histoire d'un best-seller » in *Vingtième Siècle. Revue d'histoire,* 23, 1989, 25-48.
[154] *http://discours.vie-publique.fr/notices/993002100.html*
[155] *https://www.hadopi.fr/*
[156] *https://cnnumerique.fr/*
[157] Même si d'une certaine façon, paradoxale, mais en réalité très facile à saisir comme un double effet, le numérique favorise aussi cette pédopornographie qu'elle traque. Nous y viendrons de façon plus détaillée lorsque nous évoquerons la cybercriminalité. Il y a comme un mouvement de systole et de diastole : un nouveau contrôle débouchant sur de nouvelles transgressions qui débouchent à leur tour sur de nouveaux contrôles. Cette observation est confirmée par les bitcoins dont nous reparlons plus loin.
[158] *https://www.republique-numerique.fr/*

militaire de 2013, incluant les obligations de collecte d'information des opérateurs de communications électroniques, et plus encore celle sur le terrorisme de 2014. En 2015, cette dernière est renforcée par une loi sur le renseignement. Pour autant, en matière de numérique, les résultats de la France dans l'Union européenne sont médiocres, en tout cas selon l'indice DESI (Digital Economy and Society Index) de la Commission européenne pour 2017. Le nouveau Président Emmanuel Macron et son Premier Ministre Edouard Philippe se fixent des objectifs à court terme comme les démarches administratives intégralement en ligne, ou l'accès dématérialisé à la justice. Des résultats sont d'ores et déjà constatables. Par exemple dans le secteur de l'éducation nationale, après avoir longtemps utilisé le minitel, par exemple pour mettre sur pieds les examens et les concours, l'éducation nationale a fait sa révolution internet, à différentes échelles. Des applications pédagogiques simples et bien faites favorisent l'apprentissage, et à un niveau d'exigence supérieure il est possible de découvrir des logiciels très performants. Les soins de santé publique sont mieux coordonnés grâce à la création de la carte Vitale et du dossier médical personnel, ce qui n'est pas sans entraîner des risques de non-respect de la vie privée, à conjurer par la fiabilité du système numérique concerné. Dans le cas de maladies rares, ou atypiques, ou présentant des variantes inattendues, ou encore exigeant un suivi très précis et rigoureux, des traitements longs et complexes, le numérique constitue un atout considérable. Enfin, la puissance d'un Etat tient aussi à celle de son renseignement comme l'avaient compris Sartine sous l'Ancien Régime ou Fouché sous Napoléon. Sans aucun doute les *big datas* et les *open datas* forment des ensembles de données à l'étendue hallucinante. Les Emirats pourraient s'inspirer de l'Estonie, un pays qui a opéré une véritable révolution numérique en l'espace de seulement cinq ans, parvenant ainsi à dématérialiser tous ses actes administratifs et à simplifier ainsi ses démarches. En France, les services numériques publics ne sont pas à la hauteur des serveurs privés. C'est l'inverse qui est vrai en Estonie, pays il est vrai moins étendu et moins peuplé, qui compte seulement un peu plus d'un million d'habitants. Les Estoniens ont créé en particulier une carte d'identité numérique, également disponible sur smartphone et qui concrétise toutes les fonctionnalités dématérialisées de la carte de sécurité sociale à la carte bancaire, de plus en plus plébiscitée. L'e-signature permet également de faire des économies.

c) ***Les résistances à surmonter.***

152. L'efficacité renforcée des politiques publiques se heurte toutefois à des difficultés importantes qui la réduisent. En l'occurrence, d'une part, le fait qu'une partie des populations, qui n'est pas négligeable, même en France, ne jouit pas d'une maîtrise ni même d'une aisance minimales avec les nouvelles technologies, et d'autre part, les réticences et la méfiance souvent liées d'ailleurs à l'ignorance mais pas seulement car elles peuvent se fonder sur des craintes de possibles conséquences négatives pour l'humanité ou à une répugnance psychologique, irrationnelle mas difficilement surmontable. Le numérique est un outil mais qui est loin d'être familier à tous. La limite d'efficacité du numérique ne tient pas seulement au fait que le haut débit fasse parfois défaut, ou au fait que des personnes n'aient jamais recours aux nouvelles technologies mais d'une part à l'engorgement des serveurs publics, d'usage exaspérant quelquefois, et d'autre part à la maladresse des utilisateurs. Nous assistons à un clivage géographique et générationnel entre des personnes à l'aise avec le numérique et qui en font un outil commode et souvent plaisant – avec le risque aussi de possibles addictions - et d'autres personnes en revanche qui en ont peur, ou tout simplement l'utilisent mal, de sorte qu'elles peuvent même avoir le sentiment, à l'évidence fallacieux, de l'inutilité voire de la nocivité du progrès numérique qui ne serait efficace. En fait, cette efficacité est temporaire, à cause du mauvais état du matériel par exemple, d'une maintenance insuffisante, d'une organisation en amont chaotique, ou plus généralement de l'incapacité de nombre d'utilisateurs de mettre à profit les nouveaux moyens faute de pouvoir s'en servir. Il est vrai aussi que d'un point de vue psychologique il n'est pas forcément particulièrement stimulant de s'initier à des techniques qui font un peu peur pour y déclarer ses revenus ou payer des taxes ! La motivation subjective ne s'en trouve pas forcément renforcée.

153. De façon plus fondamentale, il ne faut pas non plus attendre du numérique ce qu'il ne peut donner. Ainsi, en matière d'enseignement, il devient très facile d'accéder, où que l'on se trouve et dans un temps record, à une quantité considérable d'informations. Mais le tri de ces informations, la mise en perspective, le discernement entre ce qui est essentiel et ce qui ne l'est pas constituent toujours des conditions impératives d'une bonne utilisation et d'une vraie efficacité. Même la génération « Petite Poucette » dont parle Michel Serres[159] doit relever le défi d'une bonne intelligence des données qu'il ne suffit pas d'avoir à disposition mais qu'il faut savoir exploiter et articuler. La question n'est pas seulement de mettre à disposition des

[159] Michel SERRES*, Petite Poucette*, Paris, Le Pommier, 2012. Le philosophe fait référence à l'aisance avec laquelle les jeunes générations se servent de leurs pouces, par exemple pour envoyer des SMS.

élèves ou étudiants un bon matériau de qualité mais encore de déterminer ce que les différents acteurs du secteur éducatif peuvent en faire, et avec quelle sagacité ils s'en serviront. Des moyens grisants et une quantité d'information considérable peuvent donner le vertige, de sorte que les utilisateurs ne s'y retrouveront plus, et engendrer la confusion. Il semble évident, cependant, que l'école ne puisse faire totalement l'impasse sur la révolution numérique dans le monde actuel[160], lors même que des risques existent, par exemple d'affaiblir la capacité de concentration et donc de réflexion des élèves. L'école se doit impérativement de faire acquérir aux élèves les méthodes et aussi les codes qui se développent et s'imposent dans le monde actuel, de dégager les logiques, d'indiquer les raccourcis, et de rendre familières les nouvelles générations aux mécanismes plus complexes de la civilisation numérique, à ses forces et à ses faiblesses. On peut également estimer que l'école n'est pas simplement un lieu où sont communiqués des savoirs théoriques, ni même seulement le cadre d'un enseignement pratique. L'un des devoirs prioritaires de l'éducation en milieu scolaire, qui n'est pas une simple instruction ou un entraînement, consiste en l'éveil d'une capacité d'acquérir et de perfectionner une maîtrise éthique des nouveaux atouts[161]. L'école est un lieu d'apprentissage de la citoyenneté, autrement dit d'une capacité de se positionner de façon responsable dans le monde présent, avec ses défis et ses limites. Un citoyen responsable ne peut à l'évidence ignorer les progrès technologiques qui affectent la société dans laquelle il est appelé à vivre. C'est pourquoi, l'utopie d'une école protégée comme une citadelle du numérique – ce qui peut être une tentation pour certains enseignants, inquiets, non sans raison, des perturbations constatées et possibilités sur le travail intellectuel des élèves – ne peut être cultivée, sinon dans la mise en place d'une progressivité de la découverte et de l'acquisition de ces nouvelles pratiques.

154. Ainsi, l'accueil du numérique dans le cadre scolaire paraît bien incontournable, mais encore faut-il qu'il soit accompagné et mis en place intelligemment et prudemment par des enseignants. Cela signifie concrètement deux choses. D'une part, l'acquisition du numérique doit se faire progressivement, selon un échéancier judicieux. D'autre part, l'appropriation de ces nouveaux moyens suppose la pédagogie d'un être humain, du maître, qui éveille, guide et conseille. Ne serait-ce que pour limiter les risques d'addiction chez les uns, et chez les autres un décrochage, induisant un retard creusant encore l'inégalité entre ceux qui peuvent plus facilement acquérir

[160] Cédric FLUCKIGER, «La culture des élèves : enjeux et questions », *in Revue française de de pédagogie*, 163, avril-juin 2008, 51-61.
[161] Maurice MAZALTO, *Architecture scolaire et réussite éducativ*e, Paris, Fabert, 2008.

les nouveaux codes et ceux qui, en revanche, le peuvent plus difficilement. Paradoxalement, loin de rendre inutile la figure du maître, le numérique va à la fois lui donner de nouveaux contours, le dégager de ce qui peut-être fait par la machine, et ainsi la revaloriser dans ce qu'elle présente d'incontournable. Il nous semble d'ailleurs que cette évolution est vraie dans l'ensemble des secteurs modifiés par le numérique et des évolutions induites pour les diverses professions. D'une certaine façon, ce ne sont pas des professions elles-mêmes qui vont disparaître que certaines activités dans le cadre de ces professions. Pour prendre un autre exemple, un assistant de direction est toujours utile mais pour d'autres tâches. Dans le cadre du maître ou du professeur, cela semble singulièrement vrai et actuel. En un premier temps, cela exigera de l'enseignant un effort d'adaptation personnelle au numérique dont il ne pourra se dispenser. Il lui faudra en effet non seulement s'initier au numérique mais bien le maîtriser, car il est évident que seule une telle maîtrise lui permettra à son tour de la faire acquérir à d'autres. Il n'est bien entendu pas possible de transmettre ce qui n'est pas acquis, ni de garantir aux autres la maîtrise de ce que l'on ne maîtrise pas soi-même. Cela demandera certainement un certain temps, parfois non négligeable, un effort personnel de la part de chaque enseignant, mais un investissement financier vraiment conséquent de la part des pouvoirs publics. Des heures et des journées de formation permanente doivent être mises en place. Lorsque le recrutement des enseignants se fait par des concours (comme le CAPES et l'agrégation en France), il va de soi que la maîtrise satisfaisante doit constituer un élément de sélection, comme du reste la connaissance de la matière enseignée elle-même et les compétences plus directement pédagogiques. Il va de soi qu'une telle avancée ne peut se faire en un jour, car il faut trouver de bons formateurs pour les maîtres. Par ailleurs, ces derniers s'orientent sans doute vers l'enseignement par un intérêt pour la transmission directe à des personnes ou/et pour une matière intellectuelle dans laquelle ils font preuve d'excellence, et n'ont pas forcément un tempérament de geek, ni une grande appétence pour les technologies nouvelles. Doivent donc être surmontées des peurs mais aussi parfois même des répulsions – souvent associées aux premières il est vrai mais pas nécessairement car elles peuvent naître d'un constat réel de dommages collatéraux possibles ou réels du numérique - de la part des enseignants. Les enseignants peuvent, du reste, se sentir appartenir à une autre génération que leurs élèves, moins familiarisée à l'usage constant du smartphone que les jeunes transportent aujourd'hui avec eux. Un certain sentiment de vertige peut les inciter à garder leur distance en regard des potentialités de calcul d'un smartphone ou de la possibilité offerte aux élèves dans un temps record de vérifier une information (par exemple sur Wikipédia, ou ailleurs) et d'en savoir plus dans l'instant même que la mémoire même érudite de l'enseignant ne saurait le capitaliser.

L'aversion envers ces nouvelles technologies peut également naître du sentiment que la réflexion dans la durée, l'imprégnation progressive qui forge une culture, le discernement patient des enjeux, loin d'être favorisés par le numérique sont en fait menacés par sa rapidité et l'abondance non contrôlable des données et des informations, impossibles à trier, à structurer, à hiérarchiser et à mettre en perspective. Mais justement, les enseignants peuvent aussi estimer que ces nouvelles difficultés loin de les discréditer les rendent au contraire plus indispensables que jamais, et aussi autrement, car il leur revient justement de faire acquérir aux élèves les moyens d'un bon usage du numérique et de compléter les atouts de ce dernier par ce qu'il ne peut donner. Les enseignants peuvent ainsi, au prix il est vrai d'un effort personnel non négligeable, être les initiateurs d'une véritable « technologie de l'intellect » qui suppose une double compétence, indissociable : numérique et intellectuelle[162]. Il est opportun de souligner que l'intérêt du numérique réside principalement, au-delà du renouveau des outils, dans l'implantation de moyens fructifiant par eux-mêmes, comme un jardinier qui plante, et entretient des plantations qui d'une certaine façon grandissent et se développent toutes seules par la suite. Il va de soi que le numérique n'est pas un objectif en soi mais un moyen. Pourtant, ce moyen ne peut se répandre et se perfectionner que dans un certain contexte. Or, l'organisation actuelle de l'enseignement dans de nombreux pays, en particulier la France, ne s'y prête guère, d'abord faute de moyens mais aussi à cause de la segmentation du temps et de l'espace ainsi que d'un cloisonnement des disciplines encore trop fermées à la transversalité.

155. La question de la place du numérique dans l'éducation, notamment scolaire, est indissociable du développement actuel, encore inchoatif mais prometteur de l'intelligence artificielle[163]. Les imaginations se déchaînent car la perspective d'une intelligence artificielle forte, autrement dit capable de supplanter et de dominer les humains, sinon de les massacrer – en tout cas dans le pire des scénarios - impressionne beaucoup les mentalités. Nous n'en sommes cependant pas encore dans un scénario à la *Matrix*, du nom de ce célèbre film de cette trilogie cyber cinématographique chargé d'un lourd message philosophique sur le futur[164]. Comme le montre

[162] Jack GOODY*, La raison graphique,* Paris, Minuit, 1979 ; Pierre LEVY*, Les technologies de l'intelligence*, Paris, La Découverte, 1990 ; Pascal ROBERT, « Qu'est-ce qu'une technologie intellectuelle », *Communication et langages,* 123, 2000, 97-114.
[163] Laurent ALEXANDRE, *La guerre des intelligences. Intelligence artificielle versus intelligence humaine*, Paris, Jean-Claude Lattès, 2017 ; Gilles BABINET*, L'ère numérique, un nouvel âge de l'humanité*, Paris, Le Passeur, 2016 ; Salman KHAN*, L'éducation réinventée*, Paris, Jean-Claude Lattès, 2013.
[164] Slavoj ZIZEK, *Bienvenue dans le désert du réel,* Paris, Champs-Flammarion, 2002 ; Michaël LA CHANCE, *Matrix. Mythologie de la cyberculture*, Québec, Presses de l'Université Laval, 2006 ; Hugo CLEMOT, *Les jeux*

Jean-Gabriel Ganascia, les perspectives vertigineuses et effrayantes qui se dessinent dans la science-fiction ne sont pas prêt de se réaliser dans les trente dernières années sans doute[165]. Du reste, en attendant, comme nous le rappellent les spécialistes, il faudra déjà dix à vingt ans pour que les seuls assistants virtuels comme Siri par exemple soient performants et bien réactifs[166]. Bien entendu, le droit se doit considérer l'avenir à long terme et il semble crédible d'envisager une sorte d'alternative encore indécidable entre l'hégémonie des hommes et des robots à un horizon très lointain[167]. *Le deep learning* qui supporte certaines évolutions déjà en cours et encore à venir permettent à des machines d'acquérir des capacités étonnantes du cerveau, mais lentement et laborieusement. De plus, le danger existe véritablement, en raison justement du temps et de la difficulté de constituer de tels réseaux de neurones de les voir contaminés et viciés par des cyberattaques toujours plus adroites[168]. Plus concrètement, dans l'aménagement de l'éducation, la question peut se poser de savoir : « a-t-on encore besoin d'une salle de classe ? »[169]. Or, donc, de toute façon, pour bien des raisons, y compris des déplacement culturels, l'enseignement ne peut plus être dispensé comme jadis, et ce à très brèves échéances[170]. Les anciennes techniques pédagogiques, certes fort respectables, font de plus en plus place à des nouvelles, encore en voie d'émergence. L'un des atouts pourrait être une personnalisation de l'enseignement, pour remédier ainsi aux problèmes posés par l'inadaptation d'un nombre croissant d'élèves ou d'étudiants, rétifs à s'insérer dans un moule peut être médiocre, ou en tout cas incapable de tenir compte des différences de personnalités et de rythmes. Les surdoués sont d'ailleurs souvent les premières victimes[171]. Quoi qu'il en soit, nul ne peut aujourd'hui ignorer le développement des *Massive Online Open Course*[172], à savoir des enseignements en ligne et faciles d'accès qui par voie de conséquence forcent les enseignants *en live* à être soit plus originaux soit plus personnels, prodiguant un suivi personnalisé et circonstancié. L'interactivité devient un objectif prioritaire encore faiblement atteint. Une

philosophiques de la trilogie Matrix, Paris, Vrin, 2011 ; Jad HATEM, *Matrix, Marx et le Messie*, Paris, Orizons, 2007. Voir aussi l'ouvrage collectif*, Matrix, machine philosophique*, Paris, Ellipses, 2003.

[165] Jean-Gabriel GANASCIA*, Intelligence artificielle. Vers une domination programmée*, Paris, Le Cavalier Bleu, 2017.

[166] Yann LE CUN, http://www.college-de-france.fr/site/yann-lecun/inaugural-lecture-2016-02-04-18h00.htm

[167] Pascal PICQ, *Qui va prendre le pouvoir ? Les grands singes, les hommes politiques ou les robots*, Paris, Odile Jacob, 2017.

[168] Thierry BERTHIER, *Cyberchronique – Décomposition systémique d'une cyberattaque, dissymétries et antifragilité*, Publications de la chaire de cyberstratégie CASTEX, janvier 2014.

[169] Laurent ALEXANDRE*, op. cit.,* 151.

[170] Emmanuel DAVIDENKOFF, *Le Tsunami numérique. Education : tout va changer, êtes-vous prêts* ?, Paris, Stock, 2014.

[171] Gabriel WAHL*, Les Enfants intellectuellement précoces*, Paris, PUF, QSJ, 2015.

[172] Nicolas OLIVERI, *Apprendre en ligne. Quel avenir pour le phénomène MOOC ?,* Paris, L'Harmattan, 2016.

mutation commence. Les études seront donc de plus en plus faciles pour tous, et non plus seulement pour des étudiants estampillés ou des autodidactes acharnés. Le corrélat immédiat est une exigence nouvelle, quantitative et surtout qualitative, de la part des universités, qui seront sans cela rapidement concurrencées et peut-être discréditées, dans la mesure où elles offriraient un savoir dispensé plus laborieusement et aussi…de façon plus onéreuse, car précisément la loi de la concurrence pourrait favoriser des offres diverses *low cost*, mais intéressantes. L'apprentissage adaptatif – *adaptative learning* – devrait constituer la prochaine étape. Dans une dizaine d'années, le statut épistémologique de l'éducation pourrait se trouver modifié. Les sciences éducatives sont aujourd'hui approximatives et objets de controverses. Dans un futur proche, grâce à des algorithmes, l'ajustement de l'objectif éducatif à la personne devrait être beaucoup plus affiné. On a pu écrire que « les enseignants actuels sont à ceux de demain ce que les alchimistes du Moyen Age étaient aux scientifiques d'aujourd'hui »[173]. Grâce à l'intelligence artificielle, les méthodes d'enseignements ne seront plus tant des hypothèses souvent conditionnées par la psychologie individuelle de l'enseignant mais des fonctionnement très ajustés à partir de la mise en algorithmes de la structure du cerveau et des modes de réponse[174]. Cette révolution pédagogique devrait être d'autant plus radicale que le fonctionnement actuel de l'école correspond justement très mal à la structure du cerveau et à ses modes de fonctionnement[175].

156. Le domaine scolaire n'est pas le seul concerné. Le volume de textes juridiques existant paraît tel que des conseils donnés mais aussi des décisions prises pourraient relever de l'intelligence artificielle, avec tous les dangers également qui en découlent comme un justice implacable, inhumaine ou manipulée par l'état, ainsi que le montre le philosophe Gaspard Koenig[176]. Le projet est revendiqué d'une justice échappant(davantage à l'arbitraire, par le biais de l'intelligence artificielle[177]. Là aussi, des résistances se font très vives. Un justiciable peut se sentir terriblement frustré de voir son cas jugé par une machine. Ainsi donc l'adaptation nécessaire des services publics au numérique n'a pas grand-chose à voir avec un certain

[173] Laurent ALEXANDRE*, op. cit,* 164.
[174] Martha BURNS, http://blog.learnfasthq.com/the-neuroscience-of-learning-and-fast-forword-by-doctor-martha-burns
[175] John MEDINA, *Brain Rules : 12 Principles for Surviving and Thriving at Work, Home and School*, Seattle, Pear Press, 2009.
[176] Gaspard KOENIG*, Le révolutionnaire, l'expert et le geek*, Paris, Plon, 2015.
[177] Laurent ALEXANDRE et Olivier BABEAU, « Confions la justice à l'intelligence artificielle » in Les Echos, 16 septembre 2016.

retoilettage des façades ou une modernisation du matériel, comme de la craie remplacé par un feutre, ou comme un papier distribué laissant la place au transparent projeté. Il s'agit d'une révolution qui commence et dont il est impossible de prévoir l'importance à venir[178]. Une telle révolution peut modifier totalement, et non pas seulement de façon conséquente, l'organisation actuelle des services publics, non seulement frappée d'obsolescence, mais surtout de plus en plus concurrencée dès aujourd'hui par des solutions nouvelles, se développant de façon exponentielle. Si des pays s'accrochent de trop aux anciennes méthodes, par peur du discrédit que susciterait leur manque d'avancée dans cette révolution, c'est là où ils seront vraiment distancés. En multipliant les précautions et les garanties, le risque s'avère d'autant plus grave et douloureux de ne pas avoir pris le train en marche ? La question se pose alors de savoir si le droit a pour vocation principale de protéger, mais avec le risque de scléroser une société, ou, en revanche d'accompagner en la valorisant une évolution même discutable ou aléatoire. La réponse dépend certainement d'une vision philosophique, mais également de la psychologie personnelle. Toutefois, le droit ne pouvant être simplement le reflet des variations individuelles et collectives, il nous semble qu'il lui incombe d'accorder une attention première aux avancées des sciences et des techniques, en considérant ce qu'elles donnent d'obtenir, mais également le risque grave de les négliger, même si c'est pour conjurer d'autres risques.

157. Face aux développements présents et surtout futurs de l'intelligence artificielle, deux attitudes globales sont sans doute possibles. D'une part, une volonté d'empêcher certaines avancées de se faire au nom du principe de précaution. Avec le risque que de toute façon les avancées redoutées se fassent quand même, mais hors contrôle. D'autre part, au contraire, la volonté de contrebalancer le développement de l'intelligence artificielle par nos propres progrès personnels. Tel est le combat, entre autres en France, mais sous une forme très médiatisée, de Laurent Alexandre : éduquer les enfants, les cerveaux biologiques pour leur permettre d'être le plus complémentaires possible de l'IA, seule manière de les rendre indispensables et donc de leur assurer un avenir. Au fond, il s'agit de sortir de l'impasse par le haut. Des figures connues comme le milliardaire Bill Gates, ancien PDG de Microsoft tire le signal d'alarme. Selon eux, il convient de dresser des digues[179]. Pour Elon Musk, l'entrepreneur sud-africain d'origine canadienne à l'origine de la voiture Tesla, l'intelligence artificielle pourrait menacer la

[178] Jean-Michel TREILLE, *La Révolution numérique. Réinventons l'avenir*, Paris, Ovadia 2015. .
[179] *https://lexpansion.lexpress.fr/high-tech/intelligence-artificielle-attention-danger-meme-bill-gates-a-peur_1647411.html*

civilisation qui est la nôtre[180]. Dans une vision progressiste de l'homme, en voie de perfectionnement continu, cultivée depuis Pic de la Mirandole et relayée par Rousseau, chaque développement est considéré en soi comme souhaitable mais d'une certaine façon participe d'un continuum malgré tout[181]. Si l'intelligence artificielle doit dépasser l'homme, nous sommes en présence de ce que l'on appelle une « singularité »[182], autrement dit le franchissement d'un seuil important. D'aucuns pensent qu'en fait le développement humain et technologique ne sera pas exponentiel mais finira par s'arrêter une fois qu'un certain sommet sera atteint[183]. En tout cas l'hypothèse seule d'une intelligence artificielle finissant par écarte l'homme donne aujourd'hui le frisson. Pour l'astrophysicien Stephen Hawking, très récemment décédé, le danger existe bel et bien de machines devenant un jour plus intelligentes que l'homme et finissant par le remplacer[184]. Le philosophe Nick Bostrom[185] pense que l'intelligence artificielle a la capacité de provoquer l'extinction humaine, mais elle ne le fera pas nécessairement. Il estime qu'une intelligence artificielle poussée à son paroxysme pourrait en effet mettre en œuvre sa stratégie dans son intérêt à elle. Mais cette super-intelligence peut également nous aider à résoudre des problèmes fort complexes, y compris à l'échelle mondiale et à inventer des solutions proprement inimaginables aujourd'hui. Dans tous les cas, l'homme ne perdra rien – au contraire – à développer sa propre intelligence grâce au numérique, et aussi aux sciences cognitives. Quel que sera le scénario futur, son intérêt évident sera d'être le mieux paré par son intelligence en quelque sorte améliorée. Comment ne pas adhérer en tout cas aux recommandations de Laurent Alexandre : « Il faut que les enfants lisent beaucoup de livres et qu'ils développent leur esprit critique pour qu'ils soient au-dessus de l'intelligence artificielle et pas en-dessous. L'IA est incapable d'avoir un esprit critique et du bon sens. Pour plusieurs décennies et pour des raisons techniques compliquées. Donc c'est là qu'il faut aller. Les gens qui auront les qualités que l'IA n'a pas, auront, bien évidemment, de très belles carrières et feront des choses merveilleuses : parce qu'il faudra plein de gens pour faire ce que l'intelligence artificielle ne sait pas faire et parce que l'intelligence artificielle va considérablement augmenter le potentiel de l'humanité. Il faudra avoir un esprit critique, être curieux, être mobile, être

[180] Elon MUSK*, http://www.lefigaro.fr/secteur/high-tech/2017/07/18/32001-20170718ARTFIG00001-pour-elon-musk-l-intelligence-artificielle-pourrait-menacer-la-civilisation.php*
[181] Florence LOTTERIE, « Les lumières contre le progrès ? La naissance de l'iidée de perfectibilité ? » *in Dix-huitième siècle*, Paris, 1998, 30, 385-396 ; Thomas HURKA, *Perfectionism,* Oxford University, 1993.
[182] Ray KURZWELL*, La Bible du changement*, tr. Adeline Mesmin, Paris, M21, 2007.
[183] Jonathan HUEBNER, « A possible declining trend for worldwide innovation », in *Technological forecasting and social change,* 72, 2005, 980-986.
[184] https://webdeveloppementdurable.com/selon-stephen-hawking-lintelligence-artificielle-danger-pour-lhumanite/
[185] Nick BOSTROM*, Superintelligence*, tr.fr., Paris, Dunod, 2015.

plastique, savoir travailler en équipe, être innovant, savoir résoudre les problèmes. Il faut envoyer nos enfants là où ils vont être complémentaires de l'intelligence artificielle »[186].

Section II : Le numérique vecteur de la démocratisation.

158. Parmi les risques évoqués et les menaces brandies, il y a bien entendu, en premier lieu, ceux d'un contrôle des citoyens par une sorte de « Big Brother » comme le laisse augurer de façon apocalyptique George Orwell dans *1984,* roman d'anticipation qui fait frémir, aujourd'hui souvent en tête des ventes aux Etats-Unis ce qui donne à penser[187]. Mais il ne fait cependant guère de doute que le numérique peut largement contribuer à une démocratisation effective, aussi bien grâce à l'information disponible qu'à la participation effective aux choix faits, et non plus simplement aux plus grandes décisions ou aux élections de représentants. Mais il nous semble que la démocratisation, saluée de façon consensuelle, même si peut-être de façon pas si sincère qu'il n'y paraît, inclut ainsi une accessibilité économique proprement renforcée à des biens. En ce sens, par exemple, on peut parler d'une démocratisation des études supérieures lorsque leur coût baisse de sorte qu'elles deviennent plus accessibles à un plus grand nombre.

a) Un contrôle par le peuple

159. Le contrôle par le peuple de la vie publique passe par plusieurs niveaux. Le premier, souvent revendiqué, est celui de l'intégrité financière des représentants des citoyens mais l'idéal de transparence démocratique nous semble en réalité beaucoup plus large. Il inclut ainsi un regard sur l'ensemble des activités du secteur public, et bien entendu des budgets. Les pays nordiques de tradition protestante y semblent attachés depuis plus longtemps que les pays de tradition catholique[188]. Il y a certainement une correspondance entre une sensibilité morale et religieuse et certains modes de fonctionnement publics. En son temps, Max Weber avait établi le lien entre l'éthique protestante et le capitalisme moderne[189]. Il existe certainement un lien entre l'éthique protestante et ses valeurs d'authenticité, d'une part, et la règle de la transparence. Il n'est donc

[186] Laurent ALEXANDRE, https://www.contrepoints.org/2017/12/04/304629-laurent-alexandre-nos-enfants-complementaires-intelligence-artificielle
[187] http://www.lemonde.fr/big-browser/article/2017/01/26/1984-de-george-orwell-est-en-tete-des-ventes-aux-etats-unis_5069648_4832693.html
[188] Christophe de VOOGD, http://www.lefigaro.fr/actualite-france/2017/05/26/01016-20170526ARTFIG00187-de-voogd-la-transparence-est-liee-au-protestantisme.php
[189] Max WEBER*, L'éthique protestante et le capitalisme*, tr.fr. Jacques Chauvy, Paris Plon, 1964.

pas étonnant qu'en Suède le droit d'accès aux informations concernant l'activité des pouvoirs publics existe depuis 1766, après avoir été théorisé par le philosophe Anders Chydenius (1729-1803). Cette éthique de la transparence a certainement favorisé le recours de plus en plus systématique aux paiements par carte ou par virement, le règlement en espèce se raréfiant et tendant à disparaître, encore que depuis un an ou deux il semble y avoir un retour de ce mode de paiement. Du reste, même les déclarations d'impôts des particuliers sont considérées en Suède comme relevant du domaine public, et peuvent être connues sur demande. La France n'a pas cette tradition. La déclaration des revenus des particulier fut longtemps considérée comme indiscrète. Adolphe Thiers par exemple, au début des années 1870, fustigeait l'impôt sur le revenu comme violant la vie privée, personne ne devant être obligé de déclarer ce qu'il gagne. C'est seulement en 1914 qu'une loi l'institut[190]. Le modèle suédois est certainement assez radical mais l'unification de l'Europe tend au moins à en faire une référence dont il s'agit de s'inspirer, même si c'est d'une façon plus souple. Au demeurant, en Suède, personne ne peut exiger que son téléphone ou son adresse figurent sur quelque liste rouge : le site *hitta.se* offre au contraire à tout un chacun la possibilité de trouver les renseignements concernant un tiers. On peut cependant se demander si un tel modèle est exportable et souhaitable.

160. C'est en 1978 que la France connaît un certain tournant par l'adoption de l'article 10 de la loi no 78-753 du 17 juillet 1978 sur « le droit de toute personne à l'information (…) en ce qui concerne la liberté d'accès aux documents administratifs». Pourtant ce droit théorique semble alors voué à rester de façon globale un vœu pour des raisons pratiques. En 2002, la création du site internet Légifrance, instauré trois ans auparavant diffuse à tous les textes législatifs et réglementaires, ainsi que les décisions de justice des cours suprêmes et d'appel de droit français, à condition bien sûr que l'internaute puisse se retrouver dans un certain dédale. Du reste, depuis le 1er janvier 2016, le Journal officiel n'est plus édité en sa version papier, en application de la Loi organique no 2015-1712 du 22 décembre 2015 exigeant la dématérialisation du support, surtout pour des raisons qui tiennent au respect de l'environnement. Dans la culture contemporaine des « *Open Data* » ce site fait pratiquement figure de vestige d'un passé récent mais déjà révolu. C'est fin 2011 qu'est lancé le portail *Etalab9,* directement placé sous la responsabilité du Premier ministre, offrant à qui est intéressé pas moins de 350 000 jeux de

[190] Jean-Noël JEANNENEY, « La querelle très topique de l'impôt sur le revenu », in *L'argent caché : milieux d'affaires et pouvoirs politiques dans la France du xxe siècle*, Paris, Seuil, coll. « Points. Histoire », 2 éd., Paris, Fayard, 1984, 96-108. Aussi : *http://philippecrevel.fr/petite-histoire-de-limpot-sur-le-revenu*

données publiques, produites par les administrations d'État et ses établissements publics administratifs. En réaction peut-être à des soupçons caressés ou à des rumeurs, le Président François Hollande impose dès le premier Conseil des ministres du 17 mai 2012, une « charte de déontologie » qui stipule : « Plus généralement, le Gouvernement a un devoir de transparence». Les polémiques se poursuivent toutefois en référence à la réserve parlementaire[191]. Il s'agit en l'occurrence de subventions importantes allouées aux députés et aux sénateurs, laissées à leur pouvoir discrétionnaire. Cette réserve n'existe plus depuis le début de l'année 2018. L'affaire Cahuzac, du nom de ce ministre en charge du budget accusé de fraude fiscale et de blanchiment d'argent, rend l'opinion très sensible au risque de corruption et favorise donc l'adoption rapide des lois relatives à la transparence de la vie publique du 17 octobre 2013. Au niveau international, en guise d'exemple, on peut également évoquer l'ONG *Transparency International,* fondée en Allemagne, et présente dans de nombreux pays du globe. Elle se fixe en particulier pour mission d'éradiquer la corruption en faisant connaître les indices mondiaux comme le taux de corruption par pays. Elle tente de rendre compte du bon fonctionnement – ou non – des institutions d'un pays, et donne une évaluation des actions gouvernementales. Il est à noter qu'aussi bien sa neutralité que la justesse de ses évaluations ont fait l'objet de très vives discussions. Certains impératifs en vue de garantir la transparence en matière économique risquent de relever davantage de l'effet d'annonce ou du trompe l'œil que d'une mise en œuvre, comme, selon le magistrat Eric Alt[192] la publication du patrimoine des élus en France. En effet, ces déclarations ne sont pas vérifiées, faute de moyens juridiques et concrets d'investigation, et donc peuvent être mensongères. De plus, l'inventaire des richesses d'un élu peut l'exposer à des voleurs et mettre en péril sa sécurité. En tout cas, chaque citoyen devrait pouvoir bénéficier d'un droit d'information quant aux investigations menées et devraient pouvoir non seulement consulter facilement les déclarations mais encore émettre des observations et peut-être des signaux d'alerte. Bien entendu, la révolution numérique permet une très large diffusion des informations. Jadis, l'un des arguments invoqués était la difficulté d'imprimer sur papier des comptes de campagne. Ce n'est plus un problème aujourd'hui. Le contrôle des finances et des intérêts parfois en conflit pourrait passer aussi par une régularisation

[191] Elina LEMAIRE,
http://archive.wikiwix.com/cache/?url=http%3A%2F%2Fjuspoliticum.com%2Farticle%2FLa-reserve-parlementaire-sous-l-angle-du-droit-constitutionnel-1143.html
[192] https://www.la-croix.com/Debats/Forum-et-debats/La-transparence-vertu-democratique-2017-03-23-1200834243

plus strict du « pantouflage »[193], à savoir du passage d'un élu du public au privé, très laxiste quand cela concerne des élus et des ministres, avec des exigences déontologiques renforcées. L'éthique financière n'est pas la seule concernée. Les pratiques policières par exemple peuvent être mieux contrôlées par les citoyens. Il en va de même des décisions de justice. L'un des obstacles tient à la difficulté non plus tant de parvenir à des informations que de faire le tri et de discerner le vrai du faux, la désinformation subtile du probable. Comme le relève l'avocat Jean-Denis Bredin non sans une pointe d'ironie : « le règne de la suprême vertu exige des professionnels de la transparence. Il faut des inquisiteurs très informés pour découvrir et dénoncer les mensonges et les secrets »[194]. En ce qui concerne l'activité parlementaire, la moindre des choses semble être que chaque citoyen puisse être tenu précisément informé des votes de ses représentants parlementaires, mais également de l'ensemble de leurs initiatives et activités. Les parlementaires ne doivent plus pouvoir se réfugier derrière le rideau des « votes de groupe ». Un moyen exceptionnel semble aujourd'hui permettre un vrai contrôle : le *blockchain* à savoir un stockage et une transmission de données sans rétention de manière à former une chaîné insécable empêchant de faire disparaître au gré de la convenance les données[195]. Il s'agit d'une base de données bien spécifique qui est protégée contre la falsification ou la modification par les nœuds de stockage, et donc pleinement sécurisée. Le *blockchain* se présente ainsi comme un système qui maintient sa fiabilité même dans les cas d'attaques et de tentative de falsification. Cette technologie de stockage ineffaçable et inattaquable peut donc avoir de multiples applications, y compris pour réduire des coûts de paiement et des coût de transaction.

161. En ce qui concerne la transparence comme exigence démocratique, on peut toutefois se demander jusqu'où elle constitue vraiment une valeur. Ne risque-t-elle pas en définitive d'être inhumaine et totalitaire ? De toute manière, certains secrets doivent absolument être préservés pour le bien du pays, à commencer, cela s'entend, par le secret défense. Quant aux affaires étrangères, il va de soi qu'en matière diplomatique un secret très rigoureux doit être maintenu. On peut également se demander si une certaine dose d'opacité n'est pas protectrice, et si une traque excessive de la corruption ne finit pas par créer un climat infernal. On se souvient du

[193] Roger LENGLET et Jean-Luc TOULY*, Les recasés de la République*, Paris, First, 2015. Ce problème se pose également pour des fonctionnaires européens ou internationaux : Slimane HEMANE*, Le pantouflage des agents de la Commission Européenne*, Editions L'Harmattan, 2013

[194] Jean-Denis BREDIN*, http://www.revue-pouvoirs.fr/Secret-transparence-et-democratie.html*

[195] Billal CHOULI, Frédéric GOUJON, Yves-Michel LEPORCHER*, Les blockchains. De la théorie à la pratique, de l'idée à l'implémentation*, Paris, Ed. Epsilon, 2017

mot célèbre de Michel Audiard, dialoguiste du film « la mort d'un pourri » (1977) : « la corruption me dégoûte mais la vertu me donne le frisson ». Ne faut-il pas s'accommoder d'une certaine tolérance avec des disfonctionnements somme toute très humains ? A force d'un purisme abrupt, ne conduira-t-on pas à l'inverse, à savoir une sorte de saturation et de colère à l'endroit d'un contrôle perçu alors comme insupportable. Le balancier pourrait alors aller dans l'autre sens. Au sujet de la transparence démocratique, Lawrence Lessing nous confie cette inquiétude : « Je crains que l'inévitable succès de ce mouvement – s'il ne s'accompagne pas de la prise en compte de la complexité de l'enjeu – finira par provoquer non pas des réformes, mais du dégoût »[196].

b) Une participation active de tous

162. La démocratisation ne se réduit évidemment pas à une information passive. Les citoyens doivent participer de façon active. Autrement dit, la démocratie doit devenir davantage participative. Les citoyens ne doivent pas seulement être tenus informés du résultat mais associés aux décisions. Depuis 2016 existe en France une Charte de la participation du public qui énumère de bonnes pratiques en ce sens, déjà établies, en cours d'établissement, ou aussi à promouvoir. Les philosophes et les sociologues travaillent beaucoup cette question depuis des décennies. Il a par exemple été mis en relief la mutation importante du rôle du médecin et des autorités médicales voulue et en partie obtenue par des malades du SIDA qui se veulent partie prenante des décisions les concernant[197]. Les services publics ne doivent pouvoir déterminer selon leurs caprices et leurs seules vues la gouvernance qui est la leur. Cela vaut aussi pour les transports par exemple ou les postes, objets de critique pour des disfonctionnements. Les malades ou les usagers sont les premiers concernés. On peut donc comprendre qu'ils veulent orienter les décisions prises ou à prendre.

163. Il va de soi que les décisions à prendre implique souvent des compétences particulières, notamment techniques ou médicales. C'est d'ailleurs la raison pour laquelle les citoyens doit pouvoir non seulement avoir accès aux informations mais se former, en sciences ou en droit. Tel est du reste le sens de la Convention d'Aarhus sur l'accès à l'information, la participation du public au processus

[196] Lawrence LESSING, "Et si la démocratie se condamnait elle-même ?", *Courrier International* 1008, mars 2010, 32.
[197] Michel CALLON, Pierre LASCOUMES et Yannick BARTHE, *Agir dans un monde incertain,* Paris, Seuil, 2002. A noter sur cette question l'illustration cinématographique offerte par le film très primé de Robin CAMPILLO, *120 battements par minute (*2017).

décisionnel et l'accès à la justice en matière d'environnement, signée le 25 juin 1998 par trente-neuf États, relative à l'environnement, mais qui doit également donner l'exemple dans les autres secteurs. Cette importante convention se prolonge par des directive européenne, dont la directive 2003/4/CE, insistant sur le devoir d'information envers toute personne. D'autres directives évoquent la tenue de débats publics. En France, cette convention est reprise dans la charte de l'environnement, adossée à la Constitution et qui rappelle que « Toute personne a le droit, dans les conditions et les limites définies par la loi d'accéder aux informations relatives à l'environnement détenues par les autorités publiques et de participer à l'élaboration des décisions publiques ayant une incidence sur l'environnement » (article 7). On peut estimer, en outre, que le portail *Toutsurlenvironnement.fr* constitue une première concrétisation conséquente de la réponse française aux exigences d'Aarhus. Il convient par ailleurs de rappeler qu'en mars 2007, la directive européenne INSPIRE, rédigée par la Direction générale de l'environnement de la Commission européenne, entend rassembler un ensemble de données géographiques mais aussi associer les citoyens à des propositions. Toujours au sujet de l'environnement, les volontés du Conseil de l'Europe de réduire l'accès aux données ont été déjouées, sauf cas vraiment particuliers, justement pour permettre une participation accrue des citoyens européens. En outre, en 2012, le Tribunal de l'Union européenne précise que les ONG disposent bel et bien d'un accès à ester en justice par exemple en mettant en cause des décisions communautaires ou leurs applications. Fait ainsi jurisprudence le recours contre le règlement 149/2008 au sujet des limites maximales de résidus de pesticides dans les denrées alimentaires. Toujours est-il que la convention d'Aarhus stipule que « chaque Partie veille à ce que les membres du public qui répondent aux critères éventuels prévus par son droit interne puissent engager des procédures administratives ou judiciaires pour contester les actes ou omissions de particuliers ou d'autorités publiques allant à l'encontre des dispositions du droit national de l'environnement».

164. Au fil du temps, des critiques ont été émises sur le fonctionnement d'une démocratie représentative qui exclut de fait certaines des prises de décision. C'est déjà le cas, à cause du scrutin majoritaire et non proportionnel, de partis politiques minoritaires. Mais aussi sans doute de catégories socioprofessionnelles peu présentes, par exemple le monde ouvrier. Certaines classes d'âge ne sont pas ou guère associées aux décisions, par exemple les enfants, les personnes âgées, les jeunes. Quant aux femmes, elles se trouvent toujours dans une position minoritaire. Les décideurs politiques finissent par former une élite à peine renouvelée ou affaiblie par des retournements électoraux. Qui plus est, la brièveté des mandats, certes renouvelables, et la perspective d'une entrée dans une

nouvelle campagne, compromet le « souci du long terme »[198] et le sens de la durée. Le fonctionnement autoréférentiel du monde politique, avec une focalisation sur le court terme et sur les seuls enjeux de l'heure fait négliger l'avenir, pourtant essentiel aux yeux des citoyens qui ne peuvent s'empêcher d'y penser. En matière d'écologie, c'est évidemment ce que nous risquons de provoquer dans les décennies à venir par nos attitudes à venir qui est déterminant[199].

165. De larges pans de la philosophie contemporaine, dont le représentant le plus célèbre est le philosophe allemand Jürgen Habermas[200] insiste sur l'importance des débats et des discussions, pour que se dégage une position mieux éprouvée, plus équilibrée, mieux informée aussi. « L'éthique communicationnelle » semble nécessaire dans une démocratie[201]. Elle permet une participation de tous aux grandes décisions, tempérée qui plus est par une exigence de qualité, dans la mesure où le débat doit être argumenté et n'est pas un pur échange d'opinions brutes et arbitraires. Dans le prolongement des intuitions de Jürgen Habermas, le philosophe James Fishkin a développé un idéal de démocratie pure, avec la plus large participation de tous les citoyens[202]. Si le débat semble réservé à certaines élites, ne peut-on envisager des sondages affinés. Fishkin propose ce qu'il appelle le « sondage délibératif ». Pour motiver les participants, une rémunération également proposée. Il faut que chaque voix compte et que chaque voix puisque s'exprimer. La proposition de Fishkin a été testée plus de 70 fois dans 26 pays du monde. Son intérêt spécifique est d'éviter une participation qui puisse tirer vers le bas, à savoir, à cause de sondages insuffisamment préparés et mal élaborés de créer une déferlante de sentiments négatifs ou d'opinions « fantômes » un peu à l'instar de ce que les réseaux sociaux connaissent. Le défoulement brut et facile n'est pas la mise en place harmonieuse d'une participation démocratique. En effet, une consultation doit être préparée et bénéficier non seulement d'un bon échantillonnage mais également de questions ajustées qui poussent à réfléchir. Une anecdote amusante montre à quel point Fishkin est en réalité soucieux que toutes les catégories soient parties prenantes. Son équipe a fourni un jour un remplaçant à une fermière de l'Alabama pour traire les vaches à sa place afin qu'elle puisse se consacrer à ses activités citoyennes. C'est en 2007 qu'a eu lieu le premier sondage délibératif européen suite au rejet du projet de constitution au

[198] Pierre ROSANVALLON,*La légitimité démocratique. Impartialité, réflexivité, proximité*. Seuil, 2008.
[199] Dominique BOURG et Kerry WHITESIDE, http://www.laviedesidees.fr/Pour-une-democratie-ecologique.html?lang=fr
[200] Jürgen HABERMAS*, Théorie de l'agir communicationnel. Rationalité de l'agir et rationalisation de la société,* tr.fr. Paris, Fayard, 1981.
[201] Philippe CHANIAL, https://www.persee.fr/doc/quad_0987-1381_1996_num_28_1_1557
[202] James S. FISHKIN, *The Voice of the People: Public Opinion and Democracy,* New Haven and London, Yale University Press, 1995.

Parlement Européen avec la participation de 362 citoyens de tous pays, de toutes origines et de tous âges, sur des sujets exigeants comme la politique étrangère ou les réformes de retraites. Le cadre formel incite les participants à un fort investissement personnel, à la réflexion, à la rigueur et à l'engagement. Bien entendu, toutes les opinions s'expriment mais justement en raison du cadre, des exigences, et du caractère lucratif de la participation, le débat ne se réduit en rien à un alignement de positions mal argumentées ou passionnelles mais débouche sur des échanges de vues de bon niveau, alors même que les intervenants ne sont pas du tout des experts au départ. C'est ainsi, de façon assez stupéfiante, que la discussion prend souvent un tour inattendu, que les convictions s'affinent et se déplacent. Les présents ont le sentiment de sortir de l'ignorance, et sont enthousiastes à l'idée de continuer à le faire. Une référence est parfois faite à la démocratie athénienne de l'Antiquité, lorsque des assemblées siégeant sur la colline de la *Pnyx* au centre d'Athènes, constituées non seulement des experts mais aussi des citoyens ordinaires tirés au sort délibéraient des questions les plus délicates et prenaient des décisions. L'analogie a ses limites car la démocratie athénienne n'associait en fait qu'une partie de la population, très réduite[203]. De plus, une démocratie immédiate et délibérative était conçue au départ à une échelle réduite, et non à celle d'un grand pays, et encore moins d'un continent. Pourtant l'expérience prouve qu'au moins en complément de la démocratie représentative telle que nous la connaissons, un surcroit démocratique et qualitatif est réellement apporté. Favorisé par le numérique et les nouvelles opportunités offertes. Malgré les limites possibles de telles consultations– car elles peuvent être biaisées, certains par exemple s'y dérobant, ou sont influencés pour le coup par la façon de poser les questions – elles constituent un progrès évident. Si ces entreprises sont encore onéreuses et exigeantes en termes de personnel et d'infrastructure, cela ne devrait plus être le cas dans un certain temps grâce au numérique qui marquera là un tournant[204]. Une autre suggestion, faite par le même James S. Fishkin et Bruce Ackerman consiste à prévoir dans chaque démocratie un jour férié et rémunéré correctement par l'Etat de délibération[205]. Fishkin parle du « *Deliberation Day* ».

166. Le premier niveau de la démocratie participative est celui de la consultation. De soi, la consultation n'implique pas que compte soit tenu de l'avis donné. La consultation n'est pas forcément une confrontation, ou un choix binaire. Au-delà de la simple consultation s'ouvre alors l'espace d'une

[203] Moses FINLEY*, Démocratie antique et démocratie moderne*, tr. fr. Paris, Payot, coll. « Petite bibliothèque », 2003

[204] Helen LANDEMORE, *Democratic Reason : Politics, Collective Intelligence and the Rule of the Many,* Yale, 2013.

[205] Bruce ACKERMANN, « La journée de la délibération » in Charles GIRARD et Alice LE GOFF, *La Démocratie délibérative. Anthologie de textes fondamentaux*, Paris, collection L'Avocat du Diable, Éditions Hermann, 2010

concertation impliquant un protocole de concertation beaucoup plus élaboré. Quelquefois, la concertation de communication peut être mise en place pour donner l'impression d'une véritable consultation mais jouer véritablement le jeu et accorder de l'importance. Il s'agit d'un trompe l'œil comme un entretien d'embauche accordé alors qu'on s'est déjà décidé pour une personne. Ce type de participation, sans contenu ni profondeur, peut découler d'une bonne intention volontariste non suivi d'effet ou pire découler d'un calcul cynique pour faire illusion. Quelquefois des espaces de concertation sont imposés sans réalité pouvoir porter des résultats faute d'enthousiasme des personnes ou également à défaut de moyens adaptés. On peut songer aux conseils de quartiers obligatoires en France, depuis la loi Vaillant de 2002, pour les villes de plus de 80.000 habitants, ou de façon peut-être plus démagogique des « conseils municipaux ». Pour limitées puissent en être les résultats quant aux décisions prises[206], il n'en demeure pas moins que de telles initiatives peuvent au moins éveiller les participants au sens de leur responsabilité, et leur donner la curiosité et le plaisir de s'intéresser aux questions autour de la citoyenneté. Un type de concertation peut se présenter comme particulièrement intéressant et bénéfique, la concertation de construction. En l'occurrence l'autorité publique décide d'associer la population à un projet, pour des raisons au demeurant diverses, quelquefois en vue d'un arbitrage entre des points de vue opposés, ou pour trancher entre plusieurs options qui paraissent également convaincantes. Quelquefois la concertation se présente sous la forme d'un référendum local, où il s'agit de répondre par oui ou par nous. D'autre fois, il faut choisir un ou plusieurs projets parmi d'autres. Concrètement, il arrive qu'une concertation serve précisément à décider qu'il n'est pas temps de décider, que cela est trop risqué, ou insuffisamment consensuel. Cela peut être le cas des référendums en Italie, où l'abstention contribue à l'échec d'une réforme envisagée. On peut également invoquer l'indécision de la population pour justifier l'abandon d'un projet que l'on sait inopportun mais que l'on ose stopper de son propre chef. Au-delà de la concertation se situe ce que l'on peut qualifier d'élaboration collégiale, où les décisions sont vraiment prises ensemble, ce qui se vérifie à la fois dans le budget participatif[207] et dans la conférence de citoyens. Le budget participatif est un processus au travers duquel des citoyens de base peuvent investir une partie du budget de leur collectivité territoriale dans différents projets et initiatives. Cette nouveauté a été imaginée dans le Sud du Brésil, à Porto Alger, en 1989. Elle gagne la France seulement au début des années 2000. Le budget participatif outre qu'il permet de conjurer la corruption, le clientélisme et la création de maffias favorise une redistribution des richesses dans un

[206] Comme le souligne le rapport au Sénat d'Annie GUILLEMOT et Valérie LETARD*, http://www.senat.fr/notice-rapport/2016/r16-662-notice.html*

[207] Yves SINTOMER*, http://www.participation-et-democratie.fr/fr/content/les-budgets-participatifs-dans-le-monde?page=0%2C0%2C1*

sens plus égalitaire, au profit de communautés humaines ou de quartiers défavorisés. En résumé, par le budget participatif les citoyens sont vraiment partie prenante dans l'allocation au budget public[208]. Pour autant, cette initiative ne remplace pas totalement ni ne discrédite en tout la démocratie représentative. On peut estimer plutôt que les deux types de démocratie se renforcent alors pour de démocratie globale à l'arrivée[209]. Certes, les élus, c'est-à-dire les représentants démocratiques sont contraints de renoncer à une partie de leurs prérogatives et de leurs exclusivités, mais c'est au bénéfice de tous en définitive. On peut dans l'idée d'une autoréglementation budgétaire ainsi mise en place une progrès de la conscience morale des citoyens qui se sentent au cœur des décisions prises. Au début des années 2000 (en 2001, 2002 et 2003) à Porto Alger, des Forums Sociaux Mondiaux ont contribué à diffuser un tel budget participatif avec le soutien prudent du Fonds Monétaire International. Chaque pays et chaque ville adaptent ensuite cette intuition au contexte. Par exemple à New York l'insistance est placée sur la participation des communautés les plus marginalisées. En Europe, en revanche, cet idéal égalitariste semble quelquefois compromis par l'investissement plus actif et plus convaincant des classes les plus favorisées cette fois[210]. Pourtant, dans une perspective égalitariste inspirée de Porto Alger, des budgets participatifs se mettent en œuvre dans une dizaine de villes françaises surtout communistes[211], souvent grâce à un tissu associatif très dense, ainsi stimulé. On peut songer d'une sorte de reconversion du militantisme de jadis sous cette forme originale. Dans certaines régions, il faut relever les budgets participatifs des lycées, par exemple depuis 2005 en Poitou-Charente sous la férule de Ségolène Royal, mais aussi en région Nord-Pas-de-Calais[212]. Ces budgets permettent par exemple la construction de maisons des lycéens offrant aux jeunes de nouvelles possibilités d'actions et de travail, mais aussi une ambiance. Les plaintes et insatisfactions sont ainsi mieux gérées et parfois relativisées, car le sens du devoir civique finit par l'emporter sur l'esprit de pure revendication intéressée tandis que le réalisme gagne aussi du terrain par le constat de toutes les difficultés à affronter et l'impossibilité de remèdes miracles.

167. Quant à la conférence de citoyens[213], il s'agit d'une autre forme de décision collégiale et d'implication de tous. Ce principe est fréquemment mis en œuvre dans des pays septentrionaux afin

[208] Osmany PORTO de OLIVEIRA, *https://www.cairn.info/revue-participations-2016-1-p-91.htm*
[209] Leonardo AVRITZER*, https://www.cairn.info/resume.php?ID_ARTICLE=DEC_BACQU_2005_01_0231*
[210] Héloïse NEZ*, http://www.metropolitiques.eu/La-democratie-participative-en.html*
[211] Héloïse NEZ et Julien TALPIN, *https://blogs.mediapart.fr/edition/la-revue-du-projet/article/050214/des-formes-nouvelles-de-democratie-heloise-nez-et-julien-talpin*
[212] Julien O'MIEL et Aymeric MONGY, *http://www.revue-participations.fr/articles/2014-2-reformer-par-l-experimentation-la-reception-du-budget-participatif-des-lycees-en-region-nord-pas-de-calais/*
[213] Dominique BOURG et Daniel BOY, *Conférences de citoyens. Modes d'emploi*, Paris éditions Charles Léopold Mayer, 2005.

de tester dans la durée différents scénarios possibles pour faire émerger autant que possible un socle consensuel. Ce type d'initiatives est encore trop peu développé en France. Sans doute, en 1998, l'Office parlementaire des choix scientifiques et technologiques (OPECST) a-t-il organisé une conférence avec un nombre réduit de participants (15) sur les OGM et en 2002, la Commission française du développement durable a-t-elle organisé une conférence avec 16 citoyens au sujet des changements climatiques et la citoyenneté. D'autres conférences du même type ont suivi avant celle qui connut davantage de succès en 2012 de l'Institut Montaigne sur le type de système de santé à mettre en piste. Il faut noter que la loi française du 7 juillet 2011 relative à la bioéthique stipule que le Comité consultatif national d'éthique doive organiser des états généraux « avant tout projet de réforme sur les problèmes éthiques et les questions de société soulevés par les progrès de la connaissance dans les domaines de la biologie, de la médecine et de la santé », incluant des conférences de citoyens de toutes les franges de la société. En réalité, il pourrait s'agir en partie d'un miroir aux alouettes dans le mesure où certaines manipulations sont hélas possibles[214] et où la complexité des débats peut désorienter les participants.

168. D'autres initiatives de démocratie participative doivent cependant être saluées. Dans le Haut-Rhin, à Kingersheim, non loin de Mulhouse, le maire Jo Spiegel a mis sur pieds des conseils participatifs ainsi constitués : 40 % de volontaires, 20 % de personnes directement concernées et 40 % de citoyens tirés au sort. Les élus sont présents mais avec un devoir de réserve pour aider les citoyens à décider et non les influences. Un village de la Drôme, Saillans, est considéré quant à lui comme exemplaire pour la mise en place de commissions participatives. En définitive, au-delà des réussites et des ratés au niveau local, c'est tout une philosophie du participatif comme tel qu'il faudrait creuser, en particulier en France, et qu'il n'est pas facile de mettre sur pieds en raison d'une histoire centralisatrice et axée sur la démocratie représentative[215]. Mais la classe politique y est-elle préparée ? Et les citoyens désirent-ils vraiment s'investir dans une démocratie participative qu'il pourrait surtout revendiquer en théorie, pour mieux critiquer les politiques globalement en place ? En tout cas l'élection favorise toujours les élites sinon ceux qui sont déjà favorisés en termes de pouvoir ou de revenus. Quant à l'idée d'une démocratie participative, elle peut aussi se heurter à l'idée que la plupart des questions importantes sont complexes et font appel à des experts compétents. Ce n'est pas entièrement certain car au-delà des méandres des savoirs techniques les citoyens

[214] Thierry MENISSIER, *Machiavel ou la politique du Centaure*, Paris, Éditions Hermann, « Hermann philosophie »., 2010.
[215] Bernard MANIN, *Principes du gouvernement représentatif,* Paris, Calmann-Lévy, 1995.

concernés disposent certainement d'un bon jugement en aval, celui du savoir d'usage. Si le cordonnier sait fabriquer une chaussure et l'urbaniste dessiner des plans, celui qui porte la chaussure et celui qui cherche son chemin en voiture dans une ville ont également une compétence « d'en bas » si l'on ose dire, mais souvent frappé au coin du bon sens. Du reste, cette reconnaissance d'un certain jugement de base de tous fleurit dans le rôle accordé aux jurés d'assises par exemple. C'est en ce sens qu'en 2006 a été avancée par Ségolène Royal l'hypothèse de la confection de jurys citoyens. Le soupçon de populisme peut être caressé. En même temps, l'initiative existe dans plusieurs pays européens depuis près d'un demi-siècle. A Berlin, en 2001, de semblables Forums furent organisés dans dix-sept quartier de la ville avec une enveloppe très conséquente. Pour obtenir l'échantillon le moins partisan les personnes ont été tirés au sort. Dans un même ordre d'idée il faut mentionner les *Town Meetings* de la Nouvelle-Angleterre[216], aux Etats Unis, qui fonctionnent de façon assez fructueuse depuis le XIXe siècle. L'éventuelle participation des médias à la couverture de l'évènement dope en général les participants. Mais l'ensemble de ces initiatives précèdent l'explosion numérique qui va en maximaliser les potentialités.

169. C'est Barack Obama qui à l'occasion de ses deux campagnes d'élection et de réélection lance le thème d'une « e-mobilisation » qu'il reprend par la suite, une fois au pouvoir. Il faut dire qu'il s'appuie sur une équipe très au point dans le domaine technologique et capable d'optimiser les opportunités offertes. Internet en particulier grâce au site fort bien fait *my.barackobama.com* s'est révélé un outil très efficace d'information et de consultation, mais aussi de mobilisation. Après la victoire de ce nouveau Président se voulant en phase avec les développements technologiques de son époque, le site *recovery.gov* communique à un large public les détails de l'affectation des dépenses publiques fédérales puis le site *healthreform.gov* informe les citoyens de l'avancée de la politique de la santé. Sans aucun doute, l'objectif visé est bien d'offrir aux citoyens des critères de discernement en vue d'une participation éclairée aux décisions. Le nouvel outil numérique donne une ampleur et une portée aux anciennes initiatives de démocratie participative, plus limitées. En Argentine, le *Partido de la Red* constitue un mouvement d'opinion visant à faire décider par les citoyens eux-mêmes le vote de leurs députés. Le mouvement s'appuie sur une open source, *DemocracyOS* permettant à chacun de se prononcer sur chaque projet de loi, le député votant alors en son nom. Il est à noter qu'il existe une version française de cet *open source* qui pourrait un jour révolutionner l'idée même de démocratie. Il existe également en France une plateforme indépendante à but non

[216] David ROBINSON *Town Meeting: Practicing Democracy in Rural New England,* Boston, University of Massachusetts Pressn 2011.

lucratif créée en 2015 pour que les citoyens puissent participer en continu à des projets à toutes les échelles : locale, régionale et nationale, Demodyne[217]. Elle est accessible sur tout le territoire. En tout cas, une dynamique de démocratie participative est lancée un peu partout[218]. Pour l'heure cela semble davantage opérationnel en ville[219]. En profondeur, et sur la durée, le projet est caressé d'une vraie mutation de la société car il s'agit selon l'expression du sociologue et politologue Pierre Rosanvallon de « refaire la société »[220]. Des doutes subsistent et quelquefois la perplexité augmente toutefois sur la pureté démocratique de la démarche qui, certes, évite le différé de la démocratie représentative mais présente en revanche l'inconvénient d'une manipulation possible d'une autre nature, peut-être plus redoutable, celle induite par l'immédiateté et l'émotion.

c) <u>La démocratisation économique</u>

170. L'idéal de démocratisation économique inclut sans doute un certain nombre de questions à résoudre et de défis à relever aussi concrets que celui du juste prix dans le commerce équitable ou des règles de production. La perspective est celle d'une régulation démocratique et citoyenne des activités économiques. Cette volonté de démocratisation économique fait écho aux thèses célèbres de Karl Polanyi retraçant l'émergence progressive de notre monde et de son fonctionnement économique[221]. Selon Polanyi, l'histoire récente se caractérise par une émancipation de la monnaie de l'ensemble de l'économie réelle de sorte que le monde financier finit par se constituer comme un monde à part, influençant toutefois les autres secteurs de l'existence. Les sphères de production et de distribution des biens ne sont donc plus entre les mains de tous, et n'obéissent plus à un contrôle démocratique, mais sont dominées par des intérêts privés d'ailleurs en compétition. Toutefois, pour Polanyi, ce processus n'est aucunement irréversible et est destiné à s'inverser au travers de crises. La démocratisation économique se réalise ainsi au travers de processus institués, de règlementations et d'un

[217] https://www.demodyne.org/browse/france
[218] Loïc BLONDIAUX, *Le nouvel esprit de la démocratie. Actualité de la démocratie participative*, Paris, Seuil, La République des idées, 2009 ; René BALME et Serge RIVRON, *La démocratie participative. La participation au concret*, Paris, La passe du vent, 2009 ; Jean LALIBERTE*, Réinventer la démocratie: pour une démocratie partici.pative sans partis politiques et sans élections,* Québec, Septentrion, 2011.;
[219] Georges FERREBOEUF*, Participation citoyenne et ville*, Paris, L'Harmattan, 2011.
[220] *Refaire société,* préface par Pierre ROSANVALLON, Paris, Seuil, La République des idées, 2011.
[221] Karl POLANYI, *La Grande Transformation : aux origines politiques et économiques de notre temps*, tr. Catherine Malamoud et Maurice Angeno, Paris, Gallimard, 1983

fonctionnement bureaucratique affiné[222]. Mais c'est en particulier dans l'espace public de proximité, donc à petite échelle, que peut s'opérer une récupération de la démocratie dans le secteur économique[223]. Il s'agit de créer des liens de solidarité. En fait, ce projet était déjà caressé en 1893 par le célèbre sociologue Emile Durkheim[224]. Mais sans parvenir à un résultat concret. Il s'agit aussi de ne pas s'inscrire dans un pure logique du profit maximum, mais cela est difficile car toute initiative locale ne peut ignorer le contexte d'ensemble. On peut envisager des micro-économies fondées sur le troc (échange d'objets ou de services mais sans argent) ou encore une monnaie municipale. En ce qui concerne le troc, il pourrait être facilité par internet puisqu'il ne s'agirait plus d'échanger dans un cadre de proximité immédiate mais sur la toile. Ainsi, il existe un site *Echange Service* très fréquenté. On peut d'ailleurs concevoir comme solution limitée, partielle et temporaire au chômage et à la difficulté de trouver un emploi pour certaines catégories d'âge ou de situation, des services échangés permettant la subsistance sans verser une rémunération cachée en argent. On se souvient des jeunes filles au pair de jadis qui étaient hébergées, nourries et blanchies par une famille en échange de service. On peut parler plus sérieusement du commerce de compensation, ou du commerce bilatéral quand deux Etats procèdent ainsi par échange de biens ou de service. Les crises monétaires favorisent bien entendu le retour du troc. On peut aussi estimer qu'à l'échelle de la proximité le troc se présente avec un visage plus humain, créant du lien entre les personnes[225]. A la limite on pourrait même se demander si dans l'histoire des civilisations ce mode d'échange n'est pas dominant – chronologiquement parlant- et s'il ne reviendra pas grâce au numérique qui le permet à large échelle cette fois. Le problème pratique du troc et de l'échange est qu'il n'est pas toujours facile à mettre en place, faute de biens équivalents – ou surtout jugés tels – à échanger. Pourtant, il n'est pas tout à fait exact de dire que l'argent remplace le troc car ce la monnaie remplit un rôle social qui n'est celui de suppléance, et ce dernier survit lorsque les échanges sont monétarisés. Et parfois sous une forme implicite : la serviabilité d'un voisin lui permet d'espérer des services en retour, sans que cela soit dit *expressis verbis.* Il nous semble d'ailleurs que c'est la raison pour laquelle, même si la tendance existe en certains pays, la disparition presque totale du paiement en espèces ne saurait s'imposer par exemple pour éviter des trafics. Au contraire, grâce à internet, il serait possible au lieu de payer en argent un service d'offrir un bien équivalent. Ce que l'on appelle aujourd'hui la consommation collaborative exprime bien ce

[222] Marguerite MENDELL, https://www.cairn.info/socioeconomie-et-democratie--9782749237480-p-149.htm
[223] Laurent FRAISSE, https://www.cairn.info/revue-hermes-la-revue-2003-2-page-137.html
[224] https://philosciences.com/Pss/268-durkheim-et-la-democratisation-economique
[225] Jean-Michel SERVET, *Les monnaies du lien*, Paris, PUL, 2012.

grand retour du troc. On peut penser par exemple au covoiturage. Le chauffeur n'est pas rémunéré pour un travail mais il y a partage des frais réels, même si c'est, par commodité, au travers d'une évaluation. L'essayiste américain Jéremy Rifkin a mis en valeur une évolution qui se dessine, également liée à la mutation du monde du travail[226]. Selon lui, la notion même de travail évolue et évoluera encore considérablement, également en raison de la multiplication des robots et du développement vertigineux de l'intelligence artificielle. Dans les décennies précédentes, le monde occidental a connu le déclin des agriculteurs (secteur primaire) et des cols bleus (secteur secondaire) au profit des services, avec l'émergence d'une importante classe moyenne. Or cette classe moyenne est aujourd'hui considérablement fragilisée et redoute une baisse de son niveau de vie. Elle n'a pas du tout été épargné par le chômage et pourrait l'être encore moins lorsque l'intelligence artificielle rendra inutile bien des professions, ou du moins des tâches de ces dernières. Les logiciels et systèmes informatiques raccourcissent la chaîne hiérarchique. Demeurent toujours et se multiplient les emplois très qualifiés et bien rémunérés, à très haut niveau de compétence et qui demandent de bonnes qualités d'adaptabilité. Quant à ceux qui ne vérifient pas ces critères, et qui forment une masse de plus en plus nombreuse et perplexe, il semble urgent de les orienter vers un autre type de rapport entre l'activité et la rémunération. Ce que propose par exemple au travers de propositions souvent jugées utopiques la sociologue Dominique Méda[227]. Un tiers-secteur concernant la frange majoritaire de la société entre les purs assistés et ceux qui ont des postes de direction et des revenus très élevés formerait l'espace d'une économie vraiment démocratique. Cela pourrait inclure par exemple l'instauration d'un revenu de base, sujet cependant fort controversé. Tout un ensemble de mesures serait en tout cas à envisager pour mettre en place cette nouvelle économie collaborative , concernant tous les secteurs. On pourrait presque parler d'une troisième voie entre le capitalisme libéral et le socialisme celle d'un nouveau type d'économie que le développement du numérique permettrait enfin de voir émerger.

171. Mais tous les observateurs ne partagent pas cette analyse de fin du capitalisme et beaucoup remarquent plutôt une « ubérisation » du monde correspondant à un nouveau capitalisme, plus tonique et plus redoutable encore, peut-être. Luc Ferry[228], par exemple, estime que le web va

[226] Jeremy RIFKIN, *La Fin du travail : Ou comment l'Europe se substitue peu à peu à l'Amérique dans notre imaginaire*, tr. fr, Paris, La Découverte, 1996.
[227] Dominique MEDA*, Travail. La révolution nécessaire*, La Tour D'Aigues, éd. de l'Aube, 2011.
[228] Luc FERRY*, L'Innovation destructrice*, Paris, Plon, 2014 *; Prométhée et la boîte de Pandore*, Paris, Plon, 2015 ; *La Révolution transhumaniste. Comment la technomédecine et l'ubérisation du monde vont bouleverser nos vies*, Paris, Plon, 2016.

justement favoriser la cristallisation de nouveaux réseaux capitalistes, beaucoup plus rapides, efficaces, productifs et concurrentiels. Certes, l'évolution vers un management latéral et non plus vertical semble un acquis, encore à advenir plus largement. Toutefois, il n'implique pas une sorte de société où le gain passerait au second plan. Certes, le coût marginal zéro permis par le numérique nous introduit bien dans un autre type de société mais cela ne sonne pas le glas du profit ni de l'aventure de l'enrichissement. De même, le travail ne disparaîtra pas complètement, et ne se résorbera pas non plus en une sorte de bénévolat dédommagé par un revenu universel. C'est, qu'on s'en réjouisse ou s'en désole, le contraire qui semble se vérifier par la marchandisation d'actifs privés et de bien personnels par exemple son logement dans le cadre d'*Airbnb* ou sa voiture dans le cas *d'Uber pop*. Les professionnels de l'hôtellerie ou du transport vont finir par être distancés, même s'ils résistent encore comme les taxis frondeurs. L'offre mercantile de service grâce à des application mettrait en difficultés ces professions qui ont intérêt à s'adapter et non le capitalisme comme tel. Beaucoup de services semblent désormais gratuits mais en fait cette gratuité est largement compensée par des avantageux collatéraux pour qui a intérêt alors à se montrer – faussement – généreux et désintéressé. Jean Tirole a justement analysé ces « marchés biface »[229] : une face gratuite et une face payante plus avantageuse que la perte à cause de la gratuité. Le bénéfice se mesure souvent en termes de données collectées et échangées. Le récent scandale de mars 2018 qui a fait perdre 14% de la valeur des actions de Facebook en bourse suite à la révélation des pratiques de la société *Cambridge Analytica (CA*), accusée d'avoir récupéré à leur insu les données de 50 millions d'utilisateurs de Facebook et de les avoir utilisées pour peser dans la campagne présidentielle de Donald Trump en 2016, montre bien que le nouvel capital, immatériel, est celui des données. En réalité, nous n'assisterions pas véritablement à une sorte de démocratisation de l'économie dans un sens égalitaire mais plutôt au passage d'emplois détruits à d'autres emplois créés, mais qui ne s'adresseront généralement pas aux mêmes. Il s'agit donc d'une transition certes plus radicale, plus brutale, plus vertigineuse mais non de la disparition du modèle capitaliste en tant que tel.

172. L'un des problèmes posés est celui de la disparition du travail, ou plutôt d'un nombre important d'activités. Si d'aucuns estiment que cela peut conduire à une société des loisirs où le travail

[229] https://www.contrepoints.org/2017/01/12/277474-jean-tirole-analyste-de-concurrence

n'occupe plus la même place éventuellement aliénante[230], sinon à la fin même du capitalisme que nous connaissons dans une sorte de troisième révolution industrielle[231], d'autres au contraire comme Laurent Alexandre[232] et Luc Ferry[233] en France estiment qu'il s'agit de mirages et qu'en fait le travail va demeurer central dans la vie de l'homme, mais sous des formes adaptées au nouveau monde qui émerge, après l'épreuve décapante d'une destruction créatrice : beaucoup de choses vont disparaître mais beaucoup de choses nouvelles naître et émerger. Il ne s'agit donc aucunement de perpétuer la répartition des métiers et des tâches que nous connaissons aujourd'hui mais plutôt de redéfinir d'autres urgences et de prévoir le recyclage et la formation nécessaires pour mettre en place les métiers de demain. Les robots nous remplaceront rapidement pour des tâches du secteur tertiaire, comme celle de guichetier ou de conseiller bancaire, mais aussi pour des activités de pointe comme la chirurgie, où le risque de défaillance est moindre. Resteront alors dans l'immédiat des métiers plus manuels, souvent mal payés et peu valorisés, comme techniciens de surface ou aide-soignant, ainsi que des professions prestigieuses, brillantes, à haute qualification, qu'il faudra très bien rémunérer. Ce qui est entre le sommet et la base risque de disparaître faute d'une rapide reconversion impliquant un souci d'exigence intellectuelle accrue. Il y a là un vrai péril pour la démocratie, ou au moins un défi, mais l'illusion serait grande de vouloir conserver dans le formol le monde actuellement existant par crainte du futur. Les législations, dans un souci social, devront peut-être accompagner, la transition, particulièrement éprouvante pour ceux qui se trouvent au mauvais endroit et au mauvais moment, à savoir à exercer une profession vouée à une prompte disparition. Des solutions transitoires comme un revenu de base[234] sont de plus en plus envisagées.

---

[230] André GORZ*, Métamorphoses du travail, quête du sens*, Paris, Folio Essais, 2004 ; Dominique MEDA*, Travail, la révolution nécessaire*, Paris, éditions de l'Aube, La Tour d'Aigues, 2010.

[231] Jéremy RIFKIN*, La Troisième Révolution industrielle : Comment le pouvoir latéral va transformer l'énergie, l'économie et le monde*, Paris, Les liens qui libèrent, 2012.

[232] Laurent ALEXANDRE*, https://www.contrepoints.org/2017/01/31/279562-intelligence-artificielle-travail-dans-le-futur.*

[233] Luc FERRY*, L'Innovation destructrice*, Paris, Plon, 2014 *; La Révolution transhumaniste. Comment la technomédecine et l'ubérisation du monde vont bouleverser nos vies*, Paris, Plon, 2016.

[234] Nous n'envisageons pas ici la proposition d'un revenu universel de base comme devant constituer une solution durable et refonder l'économie, dans le sens de la disparition du travail, avancée par exemple par Jean-Marc Ferry (Jean-Marc FERRY*, L'Allocation universelle. Pour un revenu de citoyenneté,* Paris, Cerf, 1995) mais celle plus modeste et plus pragmatique d'une aide générale donnée pour négocier la transition économique et la destruction créatrice en évitant trop de casse sociale, dans une perspective libérale non de disparition du travail remplacé par l'assistanat mais de valorisation de l'initiative individuelle pour travailler autrement : cf. Gaspard KOENIG et Marc de BASQUIAT*, Liber. Un revenu de liberté pour tous*, Paris, éditions de l'Onde, 2014.

173. L'une des formes bien différente de démocratisation qui fait l'objet de très vives controverses est évidemment la démocratisation économique qui permet aux individus et aux collectifs d'échapper à l'autorité des états et des banques. Elle commence à prendre corps sous la forme du *bitcoin*[235], en l'occurrence de cette monnaie virtuelle cryptographique associé à un système de paiement pair à pair. Etymologiquement le « *bitcoin* » signifie pièce de monnaie *(bit*) qui soit une unité d'information binaire *(bit*). Le bitcoin existe en réalité depuis une petite dizaine d'années et a été inventé par Satoshi Nakamoto. L'intérêt du système est bien entendu de fonctionner sans autorité centrale ni administrateur unique mais d'une autre façon, décentralisée, comme pour les *blockchains* grâce à l'ensemble des nœuds du réseau. Sa capitalisation est considérable : au printemps 2018 de 300 milliards de dollars. Les frais de transaction sont faibles, ce qui constitue un autre avantage non négligeable et à la charge de l'acheteur et non du vendeur ce qui est finalement assez logique, et incitatif pour les commerçants. De plus une transaction ne peut être annulée, ce qui évite toute mauvaise surprise. Certes, elle n'est pas encore implantée dans le commerce de détail mais davantage dans les échanges commerciaux à distance. Il faut bien dire qu'il a surtout été utilisé par des réseaux criminels de sorte qu'il est en bonne part dans le collimateur des autorités de contrôle et de la police. Mais le fait qu'il puisse servir les délinquants ne signifie pas qu'il ne puisse être acceptable en ligne de principe de vouloir échapper à l'arbitraire de banques. Du reste, aujourd'hui, il ne sert pas tant les activités illégales que des paiements peu soupçonnables d'être délictueux. On peut même estimer qu'à défaut de constituer une monnaie au sens propre et classique du terme, le *bitcoin* est un « cryptoactif » comme l'appelle le G20 singulièrement efficace et prometteur, et voué à un très bel avenir, sinon un schéma de monnaie virtuelle très abouti, pour contestable qu'il puisse être.

174. Du point de vue économique, philosophique et politique, le *bitcoin* traduit une critique du système monétaire actuel et de l'interventionnisme des gouvernements qui d'une part aggraverait les incertitudes économiques et les fluctuations périlleuses et de l'autre empêcherait une vraie démocratie économique où chacun pourrait être le véritable et le décideur de ses activités. Ce bitcoin[236] est un réseau de paiement novateur et une nouvelle forme d'argent., que

[235] Bonne introduction : Benjamin GUTTMANN (dir.), *The bitcoin Bible. All you need to know about bitcoin*, sd., sl., 2013.

[236] Daniel ICHBIAH et Jean-Martial LEFRANC*, Bitcoin et cryptomonnaies pour les nuls*, Paris, First, 2018 ; Saifedean AMMOUS, *The Bitcoin Standard. The decentralized alternative to central banking,* Hoboken (New Jersey), 2018 ; Gilles QUOISTIAUX, *Bitcoin et crypto-monnaies. Le guide pratique de l'investisseur débutant*, Parisj, Mardaga, 2019 ;

l'on appelle une cryptomonnaie. Une cryptomonnaie[237] est une monnaie émise de pair à pair, sans nécessité de banque centrale, utilisable au moyen d'un réseau informatique décentralisé. Elle utilise les principes de la cryptographie et associe l'utilisateur aux processus d'émission et de règlement des transactions. Depuis 2008, le bitcoin ne cesse de se développer. Néanmoins, elle est régulièrement mise en cause car on l'accuse – non sans raison – de ne pas offrir de stabilité de valeur, car il lui fait défaut une valeur intrinsèque. Cette caractéristique particulière constitue de fait un frein important à l'utilisation de ces monnaies et à leur adoption à long terme. La question est effectivement de savoir si les utilisateurs sont bel et bien dans l'assurance que les paiements seront vraiment effectués avec une véritable stabilité, indispensable pour accorder la confiance. Aujourd'hui on parle de plus en plus de *stablecoins* qui constituent une innovation plus rassurante. En tout, on est spontanément porté à une régulation du *stablecoin* par un encadrement juridique très rigoureux. La confidentialité des transactions offertes doit en particulier constituer une préoccupation de première importance et de première urgence. Le gestionnaire d'actifs *BlackRock* a ouvert la porte à l'exposition d'au moins trois de ses fonds à la cryptomonnaie bitcoin. Selon des documents enregistrés auprès de la Securities and Exchange Commission (SEC), le gendarme financier américain, la société de gestion a amendé jeudi la politique d'investissement de ses fonds *BlackRock* Strategic Income et *BlackRock Emerging Markets* Flexible Dynamic Bond Portfolio, tous deux compartiments du fonds *BlackRock* Funds V, ainsi que celle du fonds *BlackRock* Global Allocation. Une attention particulière peut être accordée à *BlackRock*, qui cherche à rentrer sur le marché des cryptomonnaies, et rend les futures éligibles[238] sur le bitcoin dans l'univers d'investissement de ces fonds tout en prenant beaucoup de précautions sur ce type d'instruments. Il va de soi que les changements ou actions sur le plan réglementaire risquent d'altérer la nature d'un investissement dans les futures sur bitcoin ou de restreindre l'utilisation du bitcoin ou les opérations des places sur lesquelles le bitcoin est négocié d'une manière qui affecte défavorablement le cours des futures sur le bitcoin, ce qui pourrait impacter défavorablement un fonds. Il ne faut pas non plus minimiser le risque d'illiquidité, car les futures sur le bitcoin ne sont pas négociées de façon aussi forte que d'autres futures, étant donné que le marché des futures bitcoin est relativement nouveau. Le constat global quick s'imposer est celui d'une nouvelle industrie qui évolue rapidement et se présente donc comme sujette à divers facteurs difficile à évaluer pour le moment. Aujourd'hui, les seuls futurs sur le bitcoin dans lesquels les

[237] Jacques FAVIER, Adli TAKKAL BATAILLE*, la monnaie acéphale*, CNRS Éditions, 2017.
[238] Un future peut se définir comme un type particulier de produit financier dérivé : il permet à deux parties de mettre en place un agrément consistant à acheter (ou vendre) un actif à un prix et à une date fixés à l'avance.

fonds peuvent investir sont des futures dont le montant est réglé en numéraire (*cash-settled bitcoin futures*) négociés sur les marchés de matières premières enregistrés auprès de la *Commodities Futures Trading Commission* (CFTC), l'agence fédérale indépendante américaine chargée de la régulation des bourses de commerce où se négocient les matières premières. Le cours du bitcoin est particulièrement fluctuant et se présente donc sous l'apparence des montagnes russes. Pour donner un exemple tout récent, après avoir atteint le seuil symbolique des 40 000 dollars le 07 janvier 2021, le cours du bitcoin est descendu seulement quatre jours plus tard pour tomber à 30 000 dollars en lundi 11 janvier 2021, soit une baisse de 25%. Ces oscillations si considérables ne sont vraiment pas très rassurantes. On peut toutefois noter – toujours à titre d'exemple – que depuis le 1er janvier 2020, la valeur du bitcoin a connu une augmentation globale – bien que nullement linéaire et constante – de 21%. Signalons au passage qu'à côté du bitcoin il existe une deuxième cryptomonnaie en termes de valorisation, l'éther qui a vu, quant à lui, son cours augmenter de 50% depuis le début de l'année, malgré la correction du marché. L'avenir demeure toujours singulièrement incertain.

175. Rappelons, pour que tout soit bien clair, que le bitcoin était une monnaie virtuelle créée en 2009 par une personne non identifiée dont le pseudonyme est Satoshi Nakamoto. Contrairement aux monnaies classiques (également appelées monnaie fiat), le bitcoin n'est pas émis et administré par une autorité bancaire. Il est émis sur le protocole blockchain du même nom. Cette technologie permet de stocker et transmettre des informations de manière transparente, sécurisée et sans organe central de contrôle. Le bitcoin, comme beaucoup d'autres crypto-monnaies, est mis en circulation via le minage. Les "mineurs", des personnes réparties partout dans le monde, effectuent des calculs mathématiques avec leur matériel informatique pour le réseau bitcoin afin de confirmer les transactions et augmenter leur sécurité. En échange, ils reçoivent des bitcoins. Ils peuvent ensuite être convertis en monnaie fiat ou être échangés contre d'autres crypto-monnaies sur des plateformes d'échange. Aujourd'hui, le bitcoin est très largement utilisé dans le monde entier, même si depuis deux ou trois ans il semble se créer avec un rythme décroissant. On estime que toutes les dix minutes se créent actuellement 12,5 bitcoins environ contre 50 en 2009. Bien entendu, les pays occidentaux sont les plus entreprenants dans la création de bitcoins mais ils sont loin d'être les seuls. Le bitcoin peut se présenter de façon particulièrement intéressant pour des pays ravagés par l'inflation comme l'Argentine et le Venezuela. En revanche, certains pays interdisent l'achat et la vente de bitcoin comme le Pakistan, l'Algérie, le Bangladesh ou encore l'Arabie saoudite. Cette interdiction est néanmoins

très formelle car il s'avère bien entendu particulièrement difficile d'interdire une monnaie aussi décentralisée, que l'on peut facilement se procurer par exemple sur des sites de pair à pair[239] par exemple. De toute manière, il est fondamental de se souvenir qu'il n'existe pas de valeur officielle du bitcoin. Nous sommes seulement là en présence d'un indicateur notifiant une moyenne des cours du bitcoin sur l'ensemble des plateformes d'échange de crypto-monnaies du monde. Le cours du bitcoin est effectivement déterminé par la loi de l'offre et de la demande. A titre indicatif, le 1er janvier 2021, le cours du bitcoin s'élève à 23 759 euros.

176. L'essor du bitcoin est très lié à celui de la Blockchain[240]. Cette dernière désigne une technologie de stockage et de transmission de l'information, transparente et sécurisée, qui fonctionne sans aucun organe central de contrôle et permet donc une finance décentralisée. Elle constitue une banque de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne tout entière. Bien entendu, il existe des blockchains publiques, ouvertes à tous, et des blockchains privées, dont l'accès et l'utilisation sont limitées à un certain nombre d'acteurs privilégiés. Au fond, si l'on ose cette imagine, il s'agit d'un très grand livre comptable public, à la fois anonyme et surtout infalsifiable, ce qui en fait toute la qualité. Ce cahier est indestructible et ineffaçable ce qui est à la fois formidable et peut-être redoutable quant aux conséquences. En tout cas, il illustre une véritable prouesse logique, mathématique et informatique d'une extrême complexité et d'une extrême cohérence[241], associant la plus grande efficacité avec l'économie la plus rationnelle des moyens. La première blockchain apparaît en 2008 avec la monnaie numérique bitcoin justement. C'est un inconnu qui la met en place, se cachant derrière le pseudonyme de Satoshi Nakamoto, qui pourrait dissimuler un entrepreneur australien. Si au départ la blockchain et le bitcoin sont liés par la suite cette nouvelle technologique extraordinaire de la blockchain se prête à des utilisations plus variées, aussi bien

[239] A savoir : un modèle de réseau informatique d'égal à égal entre ordinateurs, qui distribuent et reçoivent des données ou des fichiers. Dans ce type de réseau, comparable au réseau client-serveur, chaque client devient lui-même un serveur. Cf. Lupu Mihai VU QUANG HIEU, *Peer-to-Peer Computing*, New York, Springer Publishing, 2021.

[240] BLOCKCHAIN FRANCE, *La Blockchain décryptée*, Paris, Netexplo, 2016 ; Billal CHOULI, Frédéric GOUJON, Yves-Michel LEPORCHER, *Les Blockchains. De la théorie à la pratique ; de l'idée à l'implémentation*, Paris, editions ENI, 2017 ; Alexis COLLOMB, Primevera DE FILIPPI, Klara SOK, *From IPOs to ICOs : The impact of blockchain technology on financial regulation,* SSRN, 2018 ; https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

[241] Jean-Paul DELAHAYE, *Complexités. Aux limites des mathématiques et de l'informatique*, Paris, Belin, 2006. Annonce la blockchain à venir.

au service des gouvernements que des entreprises. La blockchain fonctionne nécessairement avec une monnaie ou un *token* (un jeton) donnés au départ, dont le bitcoin est un exemple. Les transactions effectuées le sont pas blocs et chacun de ces blocs est validé par les nœuds du réseau appelés les "mineurs", selon des techniques qui dépendent du type spécifique de la blockchain. Dans la blockchain du bitcoin cette technique est appelée le "Proof-of-Work", preuve de travail, et consiste en la résolution de problèmes algorithmiques. Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau. Sans être immédiat, ce processus est néanmoins rapide : un peu plus lent pour le bitcoin et plus rapide pour Ether. Son caractère décentralisé lui ouvre des boulevards à l'échelle du monde. En général, on distingue trois sphères de son potentiel d'application. En premier lieu celle qui regarde le transfert d'actifs, surtout monétaire, mais pas uniquement monétaire car il intéresse aussi les titres, les actions ou les obligations. Entre autres. Une deuxième sphère d'application de la blockchain est comme registre, assurant ainsi une meilleure traçabilité, pérenne, des produits et des actifs. Enfin, une troisième sphère d'application est celle des contrats, à savoir de programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine par la suite. Comme on peut aisément le deviner, les nombreux champs d'application de la *blockchain* sont véritablement immenses : des banques au assurances, du secteur de la santé, à l'industrie pharmaceutique, de l'agroalimentaire au luxe (comme *supply chain*, à savoir comme chaîne d'approvisionnement très sophistiquée) , de l'aéronautique à l'automobile. Il faut sans doute aller encore plus loin et oser dire que la blockchain ouvre véritablement la voie à l'émergence d'un nouveau web, le web décentralisé, et d'une nouvelle économie numérique.

177. Les Emirats font en tout cas figure de nouvel eldorado de l'industrie blockchain[242]. Ils ont en tout cas une bonne longueur d'avance pour l'utilisation du blockchain car ils ont multiplié les initiatives blockchains particulièrement importantes et suggestives. Par exemple, les Emirats Les EAU ont lancé la Route de la Soie Numérique – le *Digital Silk Road* en anglais – une initiative visant à numériser le processus commercial et, à développer la première plate-forme d'échange de documents financiers du pays, en utilisant la blockchain. Il faut également mentionner le projet *blockchain Silsal* qui devrait améliorer la sécurité, la transparence et l'efficacité du transport et de la logistique. Dans les Emirats, il est très facile aux résidents du

[242] https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-1-introduction

pays mais également aux touristes d'acheter rapidement et en toute sécurité les principales cryptomonnaies. Il y a plusieurs façons d'acheter facilement des bitcoins aux Émirats arabes unis, et de trouver la meilleure option pour l'acheteur[243]. L'une des façons d'acheter du Bitcoin est d'utiliser les échanges cryptographiques en ligne. Les échanges sont conçus pour prendre en charge la négociation de cryptomonnaies. Avant l'achat, les utilisateurs entrent dans un processus d'identification. Le processus s'appelle KYC (*Know Your Customer*). La procédure de vérification KYC nécessite des informations sur les acheteurs (preuve d'identité, preuve d'adresse, etc.). Une fois le processus de vérification terminé, Bitcoin est transféré dans le portefeuille cryptographique de l'utilisateur. Le seul obstacle dans cette méthode est qu'il n'est pas possible de payer en espèces. Mais il y a encore une autre façon d'acheter du bitcoin aux Emirats, l'ATM à savoir la distribution de billets par guichets automatiques. Pour le moment, à notre connaissance, le premier et le seul guichet automatique bitcoin des Emirats est situé à Dubaï, la ville la plus grande et la plus peuplée du pays, au Rixos Premium Hotel de JBR, Marina, depuis 2019, qui fait payer une commission de 5%. Mais le plus intéressant est la possibilité d'acheter du bitcoin à Dubai en espèces avec un distributeur qui permet en effet aux résidents et aux visiteurs des Émirats arabes unis d'acheter, de vendre et d'échanger des bitcoins avec de l'argent, instantanément. Il est alors possible de payer non seulement en espèces mais encore en carte de crédit. Le G20 considère que le Bitcoin est un « crypto-actif », faisant ainsi référence à des actifs virtuels stockés sur un support électronique permettant à une communauté d'utilisateurs, à condition de les accepter en paiement, de réaliser des transactions sans avoir à recourir à la monnaie légale, et ce à partir d'un logiciel et d'algorithmes très sophistiqués. Le taux d'échange de la cryptomonnaie est fixé sur des places de marché spécialisées et fluctue selon la loi de l'offre et de la demande.

178. Au fil du temps, le bitcoin est plus largement reconnu comme une monnaie parfaitement légitime. On peut même se demander si elle ne forme pas une valeur refuge, un peu comme l'or, même si cela ne l'empêche pas de servir aussi de monnaie de paiement. Cette prétention a être une valeur refuge reste cependant discutable dans la mesure où elle est et demeure très volatile. De même, il est difficile de prévoir si le bitcoin peut atteindre un jour la valeur de marché de l'or.

[243] https://www.hebergementwebs.com/blockchain/comment-acheter-des-bitcoins-a-dubai-eau

179. Cette perspective économique d'une diversification des monnaies est esquissée en particulier, depuis un demi-siècle, par l'économiste autrichien Friedrich Hayek pour lequel le monopole de l'état sur l'émission de l'argent constitue un abus et une situation anti-démocratique[244]. Des banques privées devraient être autorisées à émettre des certificats ou devises ouvertes à la concurrence et négociables à des taux de change variables. Il y aurait ainsi une concurrence entre les devises, les plus stables l'emportant sur les moins stables. Le résultat serait d'une part un système monétaire efficace et de l'autre une vraie démocratisation économique. On peut se demander si le *bitcoin* ne met pas en mouvement cet espoir, de façon encore inchoative mais prometteuse. Cela constituerait également un remède à l'attitude actuelle des banques qui étendent imprudemment leur offre de crédit au-delà de leurs réserves réelles. Cela permettrait aussi, vrai progrès démocratique, aux déposants de retirer leurs fonds sur leurs comptes courants et ce à tout moment. Sans doute, le *bitcoin* ne peut invoquer l'autorité d'une institution ou d'un Etat et n'a pas la stabilité, certes relative, d'un métal, comme l'or. Sa valeur est flottante en fonction de l'usage économique et du marché mais c'est cela aussi qui pourrait lui donner son intérêt, car il est adaptable et adapté à l'économie réelle. Surtout, son bon fonctionnement ne demande pas le recours à une infrastructure, ce qui peut constituer un point faible en termes de sécurité mais indéniablement atteste en revanche d'une certaine liberté. Sa quantité maximale étant limitée, il risque moins l'inflation. Malgré les risques et les défis juridiques, le *bitcoin* pourrait donc constituer une expérience à risques mais fort intéressante et prometteuse. Certes, des économistes comme Joseph Stiglitz, plus dirigistes, pensent que le *bitcoin* sert surtout à contourner les règles, notamment fiscales, et qu'il devrait être interdit d'autant qu'il finira par redescendre et par perdre son intérêt économique[245]. Jean Tirole le considère à la fois comme dépourvu de valeur intrinsèque donc peu fiable et ne contribuant pas au bien commun, ce qui devrait inciter à l'éviter[246].

180. Un économiste américain de la renommée de Paul Krugman a même été jusqu'à dire en 2013 que le « *bitcoin* est le mal »[247]. En aval, l'évaluation des risques et des avantages semble pourtant plus prudente. Il va par exemple de soi que la compréhension du fonctionnement du protocole est un préalable pour l'utilisateur qui ne doit pas se lancer sans le connaître. *DEVELOPPER BITCOIN* Mais les défauts liés à l'utilisation ne nous semblent pas devoir être

[244] Friedrich HAYEK*, Pour une vraie concurrence des monnaies*, tr. fr., Paris, PUF, 2015.
[245] http://www.boursorama.com/bourse/actualites/
[246] http://www.liberation.fr/futurs/2017/11/30/deux-prix-nobel-d-economie-alertent-sur-les-dangers-du-bitcoin_1613646
[247]http://bfmbusiness.bfmtv.com/entreprise/les-nobel-d-economie-vent-debout-contre-le-bitcoin-1316313.html

imputés au système lui-même et ne justifient pas son abandon mais plutôt une formation éventuelle, incluant des avertissements et mises en garde. Un autre risque à prendre plus sérieusement en compte tient au fait que pour convertir la crypto-monnaie en devises, il est obligatoire de passer par une plate-forme d'échange opérée par des entreprises privées, ce qui introduit une part de vulnérabilité. C'est du point de vue éthique que les débats s'avèrent plus complexe. Le *bitcoin* favoriserait les premiers acquéreurs de la monnaie, les *early adopters* au détriment des autres, ce qui induirait une inégalité. L'utilisation possible à des fins criminelles, déjà envisagée plus haut, constitue un argument non contournable mais sans valeur absolue car dans ce cas-là il faudrait prendre des mesures plus draconiennes sur d'autres points, et faire disparaître les espèces. Toujours est-il que tous les gouvernements ne considèrent cependant pas avec hostilité et défiance le *bitcoin*. C'est par exemple le cas des gouvernements américains et allemands. Ben Barmanke, l'ancien Président de la FED estime même qu'il s'agit d'une monnaie avec du potentiel[248]. Certains avantages peuvent donc être envisagés comme ceux de la souplesse et de la versatilité, mais aussi de la rapidité, sinon de l'instantanéité. Le fait de ne pas être soumis aux plafonds quotidiens des banques constitue aussi un argument, évidemment du point de vue de l'usager. De plus, l'exigence de transparence n'est pas violée car toutes les transactions finalisées sont visibles sur une chaîne de données. Un des autres arguments en faveur du *bitcoin* est qu'il garde et même renforce sa valeur en cas de crise des autres monnaies. Il est vrai par ailleurs que la décision de Google d'interdire, à l'instar de Facebook, la publicité en faveur des cryptomonnaies a fortement fait baisser les cours du bitcoin qui a perdu en une journée le 17 mars 2018 7% de sa valeur. A la dernière heure, la campagne de *Youtube* contre le bitcoin (BTC) affaiblit et menace la cryptomonnaie mais cette dernière n'a peut-être pas dit son dernier mot.

181. Certains prédisent qu'elle va rebondir et d'autres, au contraire, qu'elle va s'écraser et être bientôt réduite à néant, ce qui est la prophétie toute récente de l'investisseur Jim Rogers, le directeur de Beeland Intérêts, également co-fondateur du Quantum Fundy et du Soros Fund Management. Ce puissant homme d'affaires pointe le talon d'Achille du bitcoin qui est selon lui de ne pas être lié à une puissance étatique qui est aussi une puissance militaire[249]. Tandis que les monnaies fiduciaires conventionnelles, quant à elles, ont le soutien des gouvernements et de leurs armées. Selon les financiers, à supposer que les monnaies numériques survivent elles seraient en quelque sorte « remises sur le droit chemin », à savoir centralisées et contrôlées par

[248] *https://www.latribune.fr/actualites/economie/france/20131205trib000799423/la-banque-de-france-demonetise-le-bitcoin.html*
[249] *https://fr.cryptonews.com/news/summer-madness-as-economists-predict-bitcoin-demise-call-it-6807.htm*

le gouvernement. A long terme, cela reste évidemment à prouver même si sans conteste la monnaie dite fiduciaire, classique ou bitcoin, repose tout entière sur la confiance ce qui est à la fois sa force et sa faiblesse. Le point intéressant de la discussion toujours indécidable sur le futur est que, peut-être, la nouveauté du bitcoin ne serait pas si considérable que cela comme le pensent Michael Lee et Antoine Martin[250]. D'un certain point de vue c'est vrai, mais des échanges économiques ont bien lieu avec le bitcoin qui semblent contredire ou poser une exception à la règle de la confiance maximale, qui veut que la monnaie la plus digne de confiance soit préférée, à savoir celle qui est garantie de façon très légale et par un Etat. Du point de vue plus rigoureusement économique, la question la plus décisive semble être celui du découplage ou non des échanges *bitcoin* avec les marchés financiers classiques, certains estiment que la séparation des deux pourrait doper le bitcoin[251]. En tout cas, les vols de Bitcoin et de cryptomonnaies stockées dans les portefeuilles numériques ne cessent aujourd'hui de se multiplier[252], attestant du développement de l'ampleur de l'inquiétant phénomène de la cybercriminalité dont nous parlons plus loin. De plus, le Japon insiste pour une meilleure régulation du marché des cryptomonnaies, en particulier afin de lutter contre le blanchiment d'argent, mais rien ne permet de penser à des règles contraignantes adoptées à l'échelle du G20, même si le « Groupe d'action financière » (GAFI) groupant des représentants de 37 pays et tirant la sonnette d'alarme face aux opportunités que présente le Bitcoin en matière de blanchiment d'argent et de financement occulte du terrorisme entend émettre rapidement des suggestions. Le Fonds Monétaire International (FMI), pour sa part, appelle les gouvernements à imposer une régulation et une supervision et à une vaste coopération internationale, pour protéger aussi bien les investisseurs que les banques. Or, ce n'est que le début d'un processus de démocratisation économique qui échappe aux banques et aux états, dont il y a fort à parier qu'il va connaître d'autres développements suite aux progrès exponentiels du numérique. Il reste que le défi éthique et juridique est considérable. Une démocratisation sauvage et incontrôlée conduit-elle véritablement au bien de tous et dans quelle mesure ? Telle est la question qui se pose dorénavant de façon de plus en plus urgente et ne semble pas imposer une réponse unanime.

[250] *https://libertystreeteconomics.newyorkfed.org/2020/06/bitcoin-is-not-a-new-type-of-money.html*
[251] *https://www.thecointribune.com/actualites/bitcoin-le-22-juin-2020-les-bitcoiners-sont-ils-des-idiots/*
[252] *thecointribune.com/actualites/vous-detenez-du-bitcoin-et-des-crypto-mefiez-vous-des-reparateurs-informatiques/*

Chapitre II : Le numérique dans l'économie et dans les relations extérieures

182. Le numérique ne permet pas seulement de mettre en œuvre une bonne gouvernance interne, mais contribue à l'articulation de la politique intérieure et de la politique étrangère. Il peut permettre aussi une collaboration et une synergie entre l'action publique et les initiatives privées qui ne sont plus posées en concurrence irréductible. Au-delà de l'essor concernant chaque domaine particulier, c'est l'articulation entre les domaines qui nous semble revêtir une vraie importance, car elle est indispensable à tout bon fonctionnement, et à l'harmonie d'ensemble. Nous vivons dans un monde connecté, et ce de plus en plus, de sorte que toutes les sphères de l'existence sont de plus en plus reliées les unes avec les autres[253]. Autrement dit, tout est toujours relié à tout, et tout renvoie toujours à tout. Dans un film français célèbre d'Alain Corneau, « Police Python 357 », de 1976 il est vrai, un commissaire à la vie privée sulfureuse, insiste sur « la cloison » qui existe selon lui, entre les diverses sphères de l'existence.

183. C'est cette cloison qui perd aujourd'hui beaucoup de son épaisseur. Mais en même temps, cette articulation de plus en plus spontanée au demeurant, entre les différentes sphères de l'existence, entre le privé et le public, mais aussi tous les secteurs bien précis, contribue à une plus forte vitalité économique, un élan en suscitant d'emblée un autre. A l'évidence, le fait de pouvoir identifier, par exemple sur les réseaux sociaux, les centres d'intérêt des uns et des autres, les domaines spécifiques des uns et des autres, les achats potentiels et privilégiés, favorise-t-il l'économie et le commerce, tout en posant des questions éthiques et juridiques, sur la légitimité d'une telle connaissance des goûts privés des uns et des autres. En aval, c'est la question de la mercantilisation des données, lesquelles données deviennent en quelque sorte la richesse fondamentale, que l'on ne peut éviter de poser. En tout cas, au fil de l'histoire il y a des tournants, et le numérique nous fait entrer dans une nouvelle économie.

[253] Manuel CASTELLS, *Dans quel monde vivons-nous ? Le travail, la famille et le lien social à l'ère de l'information*, Paris, Paris, Fayard, 2001.

Section* I *: La nouvelle économie du numérique

184. Cette connexion de plus en plus générale se manifeste en particulier dans l'internet des objets[254]. Depuis la baisse du coût des capteurs numériques, de plus en plus d'objets sont connectés au net, et ce de plus en plus facilement, quelquefois et même souvent, sans que leurs utilisateurs n'en ait même l'idée, ce qui pose un véritable problème éthique et déontologique. Ils émettent de la sorte des informations sur leur environnement qui sont souvent exploitées par les entreprises, dans des buts mercantiles, du moins pour le moment. Il nous faut ici faire référence à l'internet des objets.

a. ***L'internet des objets et ses enjeux*.**

185. En 2017, on compte dans le monde environ 11,2 milliards d'objets connectés. Certains pays saisissent d'ores et déjà l'opportunité ainsi offerte, et parfois avec enthousiasme, comme la Chine. Parfois, ils se spécialisent dans un secteur, ce qui est le cas de l'Allemagne qui privilégie le secteur automobile et l'industrie. Il faut dire que l'avènement des voitures autonomes[255] constitue une opportunité exceptionnelle et très prometteuse, malgré des risques et des cas concrets à élucider : par exemple que fera une voiture si elle doit éviter une vieille dame qui traverse inopinément, mais qui alors se fracassera contre un arbre, entraînant peut-être la mort du conducteur ? Comment accepter un choix rationnel entre deux vies opéré par une machine, intelligente certes, mais qui n'est pas humaine. Faut-il alors laisser le choix au conducteur de se sacrifier ou non ? Sans aucun doute, lorsque la voiture autonome aura acquis un certain stade de perfectionnement, il y aura de toute façon beaucoup moins de risques d'accident, et par conséquent de nombre de morts. Le choix à faire entre telle ou telle vie devra être fait de plus en plus rarement, et sera presque totalement évité. La voiture autonome conduit à davantage de sécurité. Mais la conduite automobile peut aussi être un plaisir et un sport dont d'aucuns auront du mal à se priver. Les enjeux de ce qui constitue certes un progrès ne sont jamais minces.

---

[254] Vaste bibliographie surtout en langue anglaise : Hakima CHAOUCHI, *The Internet of Things*. London, Wiley-ISTE, 2010 ; Hervé CHABANNE, Pascal URIEN et Jean-Ferdinand SUSINI, *RFID and the Internet of Things,* London: ISTE, 2011; Olivier HERSENT, David BOSWARTHICK et Omar ELLOUMI, *The Internet of Things: Key Applications and Protocols*. Chichester, West Sussex, Wiley, 2012; Rolf H. WEBER et Romana WEBER*, Internet of Things : Legal Perspectives*, Berlin, Springer, 2010; Honbo ZHOU, *The Internet of Things in the Cloud : A Middleware Perspective*, Boca Raton, CRC Press, 2012.

[255] Georges DOBIAS, *Vers la voiture autonome : circulation et sécurité*, Paris, Odile Jacob, 2017.

186. L'Italie cultive quant à elle une certaine originalité, développant le marché du *smart metering*[256], à savoir de la comptabilisation des flux au service d'un équilibrage des réseaux, notamment électriques. Les foyers sont désormais de plus en plus souvent munis d'un compteur mesurant en temps réel la consommation, ce qui évite toute mauvaise surprise. Du point de vue plus philosophique, il y a bien entendu quelque chose de vertigineux dans cette connexion non plus entre personnes, mais directement entre objets désormais, comme si ces derniers prenaient leur autonomie, sinon leur revanche. Ce nouvel espace qui s'ouvre va susciter de nouvelles formes de concurrence et de rivalité. On peut envisager, du reste, la création d'une plateforme visant à coordonner et à réguler l'internet des objets, pour le bien des personnes qui ne sauraient faire les frais du développement technologique. De nombreuses machines sont efficacement surveillées et contrôlées en temps réel par des capteurs, comme les moteurs d'avion. La gestion peut en être faite à distance, grâce au transit immédiat d'une grande masse d'information, transit qui constitue justement l'un des atouts principaux. Le passage obligé par un relai humain peut rendre plus problématique le contrôle. En revanche, comme nous l'avons dit plus haut, deux voitures qui se réguleraient l'une sur l'autre éviteraient plus facilement une collision[257]. Il semble difficile d'éviter de façon absolue toute catastrophe mais beaucoup d'entre elles pourraient l'être. Des villes fonctionneraient au quotidien, très efficacement, et en évitant les déficits, bien mieux qu'au travers d'intermédiaires humains. Cela est singulièrement le cas pour tout ce qui relève de la domotique[258], à savoir de l'ensemble des techniques de l'électronique, de la physique du bâtiment et des télécommunications utilisées dans les bâtiments, assurant, entre autres, la centralisation du contrôle des différents systèmes et sous-systèmes aussi bien des habitations privées que de l'entreprise, du chauffage à l'ouverture et fermeture des portes ou des volets. La domotique est quelquefois appelée *smarthome*, ou maison intelligente. Elle entend bien offrir des solutions techniques afin de répondre aux exigences en matière de confort, de sécurité ou de communication, notamment dans certains cadres privilégiés comme les hôtels. Il devient ainsi possible de gérer les éléments naturels, la lumière, la chaleur ou l'eau, de mettre en marche ou d'arrêter climatisation et ventilation en fonction des fluctuations de la température, d'éviter des catastrophes comme par exemple un lavabo ou une baignoire qui

[256] Adnane KENDEL et Nathalie LAZARIC, « The diffusion of smart meters in France. A discussion of the empirical evidence and the implications for smart cities », in *Journal of Strategy and Management*, 8, 3, 22 août 2015.

[257] Charlie OSBORN*, Intel Launches automotive security board to tackle connected car security risks : https://www.zdnet.com/article/intel-launches-automotive-security-board-to-tackle-connected-car-security-risks/*

[258] Cédric LOCQUENEUX*, Le Guide de la Maison et des Objets Connectés*, Éditions Eyrolles 2016 ; François-Xavier JEULAND*, La Maison communicante,* Éditions Eyrolles, 2012 ; Edmond-Antoine DESCAMPS*, La Domotique,* Paris Presses universitaires de France, Collection « Que sais-je ? », 1988.

débordent, d'arroser une pelouse en cas d'absence, de recharger certains appareils électriques comme des ordinateurs, d'assurer une surveillance maximale à une porte, mais également de compenser des situations de handicap et de dépendance. Ces nouveaux dispositifs permettent également d'honorer certaines exigences juridiques. Ainsi, le chauffage doit-il être coupé lorsqu'on ouvre une fenêtre afin de lutter contre le gaspillage. Certains appareils peuvent également être mis en marche ou coupés à distance en l'absence des personnes. Au Japon, le Sekisui *Chemical Group* vend déjà des logements sans frais d'électricité et de chauffage. Toutefois, la domotique ne reste pas cantonnée à l'intérieur de la maison, malgré son étymologie, car *domus* en latin veut dire « maison », mais aussi, sans doute, tout ce qui s'y rattache. Elle peut ainsi mettre en relation des habitats entre eux, avec un immeuble entier, notamment sous la responsabilité d'un syndic, ou même le reste de la ville. Cela est particulièrement utile en cas d'alarme. En France, depuis une vingtaine d'années, des organismes HLM pouvaient ainsi contrôler et suivre à distance ce qui se déroule dans les immeubles qui dépendent d'eux. Au Canada, de nombreux immeubles collectifs avec un nombre conséquent de copropriétaires sont ainsi bien gérés, avec des frais minimum. Au plan financier, dans le cas d'une nouvelle construction, on peut estimer que le coût supplémentaire de la domotique correspond à un ajout de 5 à 10 % de l'ensemble des frais de constructions, pour des gains éventuellement importants, par exemple en cas d'économies d'énergie et de toute façon de moindres investissements ailleurs, dans des équipements classiques ou de personnel (par exemple de gardiennage). En réalité, les bienfaits de la domotique se font ressentir en particulier lorsqu'une coordination est assurée entre de très nombreuses fonctions. Cela traduit l'élaboration de véritable scénarios englobant ainsi tout ce qui doit être fait, et souvent de concert, dans une maison, un matin, ou sur une journée, de l'ouverture des persiennes au grille-pain. Lorsque le système est très complet et bien coordonné, c'est une vie bien plus confortable qui se présente à l'habitant, lequel habitant voit son esprit dégagé de bien des soucis. Il jouit d'une protection maximale par exemple contre les intrusions mais également contre les sinistres tels que des incendies, déjoués en amont. Des activités fastidieuses comme le ménage ou la cuisine non seulement deviennent alors plus aisées et mieux acceptées mais permettent également une grande qualité dans leur propre exécution et plus de créativité (surtout en cuisine). Au demeurant, c'est en particulier en regard des personnes handicapées et dépendantes que la domotique revêt une importance cruciale, par son rôle de compensation de l'inégalité liée au handicap et induite par lui. En France, la loi du 11 février 2005 pour l'égalité

des droits et des chances[259], la participation et la citoyenneté des personnes handicapées insiste sur la mise en œuvre d'actions d'amélioration du cadre de vie prenant en compte tous les environnements, produits et services destinés aux personnes handicapées et mettant en œuvre des règles de conception conçues pour s'appliquer universellement. Une interface doit être soigneusement constituée entre l'utilisateur et le système domotique, que l'on désigne sous l'appellation « contrôle d'environnement ». A partir de cette interface, les effecteurs peuvent agir. Il s'agit d'appareils et de moteurs pour gérer différentes fonctionnalités comme le lit, le téléphone, la télévision, l'éclairage ou le chauffage, et ce à distance et de façon nuancée. Se constitue ainsi un espace, celui de l'habitat communiquant, bien entendu agréable et confortable pour tout un chacun mais devenu indispensable pour certains. L'interface entre l'homme et la machine ne passe plus nécessairement par un écran et un clavier, mais par la voix, grâce à la reconnaissance vocale, par des murs ou autres surfaces tactiles, par des badges, par des mouvements de la main. L'objectif ne s'avère pas simplement de réaliser des opérations adaptées mais encore d'éviter de perdre du temps sur l'interface homme / machine, grâce en particulier à des algorithmes évolués.

187. En politique, la protection et l'insertion des handicapés passe par une stratégie d'autonomisation[260]. En France, par exemple, le sort des handicapés est devenu de plus en plus crucial. Il devient impensable d'envisager une infrastructure ou une organisation sans en tenir compte. En juillet 2002, le Président de la République Jacques Chirac annonce vouloir faire de l'insertion des personnes handicapées l'un de ses trois chantiers du quinquennat. Trois ans plus tard, en 2005, il décide d'adopter une loi en ce sens. Les décisions françaises sont très significatives des mesures rendues nécessaires par le sort des handicapés, dans le sens d'une reconnaissance de leur dignité, et donc dans le but de leur permettre de mener la vie la plus digne et la plus normale possible. Cela inclut donc l'accessibilité pour tous les domaines de la vie sociale mais également, aussi bien l'éducation, la formation, le commerce que ce qui en est la condition, les transports. Les techniques semblent permettre de compenser la limitation induite par le handicap. Cela vaut surtout pour le handicap physique, le cas du handicap mental

[259] *https://informations.handicap.fr/decret-loi-fevrier-2005.php*

[260] Bob SAPEY, « La politique du handicap : un modèle reposant sur l'autonomie individuelle » in *Informations sociales* 2010/3, 128-137. Louis BERTRAND, « Politiques sociales du handicap et politiques d'insertion : continuités, innovations, convergences « , in *Revue des politiques sociales et familiales*, 2013, 43-53.

étant bien entendu plus compliqué. En tout cas, les acquis et les promesses du développement technologique semblent pouvoir constituer une aide considérable.

188. Les nouveaux dispositifs permettent également aux personnes âgées de rester chez elles, dans une certaine autonomie, et sans les dépenses d'une aide à domicile trop présente. Chacune des opérations de la vie quotidienne devenant plus facile en réalité, sinon automatique, beaucoup de dangers pouvant être conjurés comme le gaz allumé et oublié, ou éteint tout en fuyant, les personnes âgées peuvent rester dans leur appartement ou même leur maison. Or, pour elles, cela représente souvent un élément de confort et de bien-être assez considérable. "On ne déracine pas les vieux arbres sans conséquences".

189. Outre l'aspect financier, qui est - bien entendu - loin d'être négligeable (en particulier pour des familles qui devraient prendre à charge les frais de maisons de retraite, souvent fort chères, surtout si elles sont médicalisées), il convient de placer l'accent sur l'aspect humaniste. En effet, en général - même s'il y a des exceptions – les personnes âgées aiment rester chez elles. C'est un traumatisme - une sorte de "première mort" - de devoir le quitter. La téléassistance se présente donc comme un bienfait considérable ; dans la mesure où la dimension sociale ne doit pas seulement tenir compte des aspects économiques, mais également des aspects psychologiques, existentiels et humains. De même, en matière de sécurité, la domotique va devenir de plus en plus indispensable ; particulièrement pour prévenir les incendies ou les cambriolages. Les détecteurs de fumée sauvent des vies. En amont, il devient possible de prévenir davantage les cambriolages. Les techniques modernes permettent de sécuriser les portes, de mettre en place des alarmes et de les relier à des centres de surveillance[261].

190. Elles permettent de filmer les délinquants, de les pister et de les arrêter plus facilement. En matière de prévention contre les cambriolages, on peut évoquer les détecteurs de mouvements qui déclenchent une lumière extérieure ou une alarme à l'intérieur du domicile, mais il ne faut pas négliger non plus les simulateurs de présence. Ceux-ci doivent être plus sophistiqués que la simple lumière restée allumée (ou la radio en marche). Ce qui, du reste, peut également susciter la critique, sans compter la dépense d'énergie, ou des risques d'incendie. On sait que des appareils simulent la réponse à l'interphone, même en l'absence, tout en pouvant aussi, bien entendu, déclencher divers appareils ou des veilleuses en alternance.

[261] Amandine SOURD et Vincent DELBECQUE, « Le rôle des éléments de sécurité face aux cambriolages », in *Grand Angle*, 40, décembre, 2016.

191. Du point de vue de la protection de l'environnement, le bénéfice peut être considérable également. Les économies d'énergie peuvent être très importantes. L'autoconsommation (à savoir, la consommation de sa propre production d'énergie) permet de générer des économies considérables en la matière. Tout le monde sait bien qu'aujourd'hui des panneaux photovoltaïques peuvent servir à produire de l'électricité à partir du rayonnement solaire. Par la suite, l'énergie captée peut être utilisée dans le cadre domestique, ou revendue totalement ou partiellement à un fournisseur d'électricité. Bien entendu, pour qu'il y ait une vraie rentabilité, il faut veiller à trouver judicieusement l'endroit où placer ces plaques, plutôt plein Sud qu'au Nord. Les panneaux doivent avoir également un certain type d'inclinaison. Il va de soi que l'autoconsommation n'empêche pas, en complément (ou simplement par précaution, en cas de problème) le raccordement au réseau.

192. Pour davantage d'autonomie en matière d'autoconsommation, il semble opportun de disposer de bonnes batteries. Elles assurent le stockage en journée, afin de pouvoir réutiliser en différé l'énergie reçue. Hélas, elles sont encore très chères aujourd'hui. De sorte que le budget initial s'avère fort important, mais rentable sur le long terme.

193. Les pièces peuvent demeurer à température constante. Ce qui est meilleur pour la santé et évite la gabegie de chauffages "allumés et coupés", engendrant une perte importante - à chaque fois - d'énergie pour réchauffer à nouveau la pièce.

194. Cela vaut également pour la climatisation[262], bien entendu. Les prochains étés s'annoncent "caniculaires", comme le laisse augurer l'été 2018 en Europe occidentale. Ce qui s'accompagnerait, d'ici quelques décennies peut-être, de températures beaucoup plus élevées[263]. La question du réchauffement climatique, de plus en plus brûlante – sans mauvais jeu de mot, suscite bien des débats et bien des controverses : en particulier, à cause de la pollution par l'homme (CO2).

195. Nous ne pouvons pas ici aborder ce sujet vaste et délicat. Néanmoins, le développement de la climatisation semble bien à l'ordre du jour. Ceci, malgré les innombrables problèmes que cela pose pour l'environnement (en raison de la consommation énergétique excessive que cela

[262] Francis MEUNIER, Paul RIVET, Marie-France TERRIER, *Production de froid, Froid industriel commercial, domestique et conditionnement d'air*, Paris, Dunod, 2015.
[263] Comme le note, avec modération et prudence toutefois, le Rapport Jouzel*, le climat futur en France* : http://www.meteofrance.fr/climat-passe-et-futur/le-climat-futur-en-france

implique), surtout lorsque l'usager est peu soucieux de l'environnement. Depuis la moitié du XIXe siècle, l'idée d'une climatisation systématique et bien organisée s'est renforcée.

196. Elle fut rendue possible grâce à l'inventeur James Harrison. C'est seulement en 1902 que la climatisation moderne est inventée par Willis H. Carrier en 1902. Si la taille des compresseurs a beaucoup diminué depuis le temps, la climatisation continue à poser des problèmes de consommation importante d'énergie. Chaque année, la consommation énergétique est en hausse. Aujourd'hui, le phénomène s'accélère. Elle devrait véritablement exploser dans le futur. Cela tient, d'une part, à une certaine augmentation des températures, mais également à une difficulté toujours croissante des individus à supporter des températures désagréables, ainsi qu'à une exigence plus grande de confort, ou à d'autres raisons comme, par exemple : un confinement tel que celui connu au moment du pic de la crise sanitaire du coronavirus.

197. Or, une bonne climatisation ne se soucie pas seulement de la température, mais également du taux d'humidité de l'air. Elle inclut donc des fonctions d'humidification et de déshumidification. En outre, des impératifs hygiéniques doivent être soigneusement cultivés. Il faut veiller, par exemple, à la fibration de l'air soufflé. Différents systèmes de climatisation existent, plus ou moins gourmands en matière de consommation énergétique.

198. La climatisation pose des problèmes juridiques, en raison de risques sanitaires qu'elle peut faire courir, parfois plus graves que ceux liés à une température non maîtrisée : à commencer par des refroidissements, mais également des infections plus sérieuses par des agents pathogènes, y compris la légionellose ou le récent Covid-19. On ne peut oublier le problème des allergies et de l'effet possible des désinfectants très agressifs.

199. Toutefois, c'est surtout pour l'environnement que se posent les problèmes les plus sérieux. En effet, elle augmente fortement la consommation énergétique des bâtiments ou véhicules qui en sont équipés. Ce qui n'a pas qu'un inconvénient pour les particuliers. La climatisation utilise souvent des dispositifs frigorigènes utilisant des gaz à effet de serre : 2 000 fois supérieur à celui du CO2. Ce qui est considérable, et n'est pas sans impact sur le réchauffement climatique global et la montée des mers.

200. Pour éviter de tels dommages collatéraux, il est quelquefois suggéré d'opter pour une sorte de climatisation passive, avec des maisons ou des véhicules mieux conçus en amont. Il ne faut d'ailleurs pas oublier d'autres options alternatives comme : le rafraîchissement par évaporation d'eau (dans les rues des villes par exemple), même si les résultats s'avèrent à l'arrivée bien

moins importants que prévus. Au sujet de la climatisation, le législateur se doit de tenir compte de tous ces facteurs. La législation progresse en effet, et heureusement.

201. Il s'agit, en particulier, d'appliquer le protocole de Montréal[264] sur la protection de la couche d'ozone. Celui-ci interdit l'utilisation de certains gaz. Ce protocole se présente comme un accord international qui fait suite à la Convention de Vienne, sur la protection de la couche d'ozone de mars 1985. Il naquit d'une inquiétude entraînée par l'amincissement inquiétant de la couche d'ozone. Signé par 24 pays et par la Communauté économique européenne, le 16 septembre 1987 dans la ville de Montréal, au Québec, il est entré en vigueur le 1er janvier 1989.

202. En 2009, 196 pays sont signataires de ce Protocole. Ce qui en fait le premier protocole environnemental à atteindre la ratification universelle. Bien entendu, la législation intègre aussi les exigences encore plus drastiques du traité de Kyoto, mais de façon progressive, et quelquefois délicate. Il convient de signaler - en particulier - la directive européenne sur la performance énergétique des bâtiments. Celle-ci prévoit une inspection périodique des systèmes de climatisation et des pompes à chaleur réversibles d'une puissance supérieure à 12 kW (hors « froid industriel » soumis à d'autres réglementations). Les inspections doivent être soigneusement renouvelées au moins une fois tous les cinq ans.

203. En France, un nouveau décret n° 2007-363 du 19 mars 2007, interdit le fonctionnement des climatiseurs lorsque la température des locaux est inférieure (ou égale) à 26 °C. Elle ne peut se justifier que pour des raisons médicales[265].

204. Depuis le 4 juillet 2009, les spécialistes de la climatisation et de réfrigération doivent présenter - en bonne et due forme - une attestation de capacité. Malgré les restrictions apportées et souhaitées, dans de nombreux pays émergents, l'augmentation du revenu d'un foyer les pousse, à cause des conditions climatiques, à programmer l'achat d'un climatiseur. Des milliards de nouveaux appareils sont susceptibles d'être installés d'ici 2050. Ce qui est considérable. Cela s'ajoute aux nombreux réfrigérateurs existants, l'un ne remplaçant pas l'autre. On peut alors imaginer, avec effroi, la quantité d'émission de gaz à effet de serre. D'ici 2050, on peut légitimement redouter le doublement de la quantité émise. Ce qui est considérable.

205. L'urbanisation rapide de nombreux pays risque encore d'accroître ce phénomène. Face à cette menace de plus en plus urgente : il faut promouvoir et faire connaître des alternatives. Sans

[264] *http://ozone.unep.org/Publications/MP_Handbook/MP-Handbook-2012.pdf*
[265] Version en vigueur au 29 mai 2022 : Légifrance

quoi, les interdits finissent bien par être contournés. En 2017, un polymère hybride de fibre de verre, traité avec une fine couche d'argent, a été lancé. Il vise à offrir une isolation très fiable.

206. De toutes les façons, en ce qui concerne le combat, en amont, contre la dépense énergétique excessive, des aides à la rénovation du logement peuvent, par exemple, être mises en place. Il se peut aussi que la législation devienne encore plus contraignante ; quitte à augmenter ces aides, ou l'assistance et le conseil. Le bénéfice se retrouve ensuite en aval, au bout du compte.

207. Certes, des résistances existent toujours face à l'idéal d'une maison connectée. La principale tient à l'accent mis par les Français sur le rapprochement avec la nature, plutôt que les satisfactions apportées par la maison elle-même.

208. En outre, pour le moment, la technologie de la domotique coûte en général cher. Cependant, le prix devrait rapidement baisser. Il semblerait que ce type de produit finisse par être plébiscité par tous les foyers : qu'il devienne incontournable aux yeux du plus grand nombre. Il est également vrai que les fluctuations, les menaces économiques, l'incertitude dans la vie professionnelle ne favorisent pas l'investissement dans des équipements très perfectionnés, rentables à long terme. Les rumeurs, fondées ou délirantes, concernant l'influence délétère des ondes sur notre santé (par exemple sur les cancers), dissuadent aussi de se lancer dans certaines aventures technologiques jugées risquées. Enfin, le sentiment existe également du caractère intrusif de ces nouvelles technologies.

209. L'Internet des objets ouvre également des lendemains qui chantent en raison des possibles applications industrielles. Leur ampleur est aujourd'hui difficile à évaluer. IBM investit des milliards dans une *Business Unit* mondiale (constituée de plus de 2 000 consultants) et dans le programme informatique *Watson*, destiné à superviser et contrôler les connexions de l'Internet des objets. Le développement de l'Internet des objets est étroitement lié à l'augmentation considérable du nombre de données que l'on trouve sur le réseau, et qui se trouve à l'origine du Big data.

210. Le champ d'application de l'Internet des objets est au demeurant presque illimité. Les anciens obstacles techniques (comme la nécessité d'une connexion au réseau télécom) étant levés, le développement de l'Internet des objets pourrait bien s'avérer exponentiel. En France, de nouveaux réseaux ont été créés. Ils relèvent d'un protocole technique simplifié, beaucoup plus

efficace, de bas débit (économe en énergie), et de longue portée. L'objet communique ses informations de façon tout à fait autonome.

211. Ainsi, dans l'hexagone, la société SIGFOX, dotée aujourd'hui d'ambitions mondiales, s'impose comme un opérateur en plein développement. Les problèmes éthiques posés par l'Internet des objets ne sont pas négligeables. Ils sont les mêmes que ceux posés globalement par le développement du numérique. Toutefois, une dangerosité supplémentaire doit être signalée. Elle tient à la vulnérabilité de la machine[266], mal protégée. Celle-ci est une cible de choix des hackeurs qui en feront une sorte de "tête de pont", favorisant des attaques plus redoutables encore. Il semble évident que plus le nombre des objets connectés augmente, plus de telles attaques seront à redouter, et seront fréquentes. En effet, nombreuses vont être les failles de nos systèmes[267].

212. En définitive, tous les objets connectés de l'Internet des objets sont des sortes d'ordinateurs qui devraient être traités comme tels. Or, ils ne le sont pas - pour des raisons surtout économiques. De sorte qu'ils constituent des portes d'entrée pour des attaques cybernétiques parfois très importantes. C'est ainsi le cas d'un "*smart-aquarium*", connecté à l'Internet dans un casino nord-américain, qui a récemment été utilisé pour exfiltrer des données du réseau de l'établissement. Cet aquarium, relié au réseau interne du casino, se connectait en direct (VPN) vers l'extérieur du bâtiment, offrant ainsi un point de vulnérabilité trop ignoré. Un autre exemple peut être mentionné : une université aux États-Unis a été complètement déconnectée de l'Internet lorsque des pirates informatiques ont exploité plus de 5.000 de leurs "*Smart devices*", tels que des ampoules et des distributeurs automatiques, pour mener des attaques en ligne. Il a suffi d'une toute petite faute dans la configuration pour faire vaciller l'ensemble du système.

213. Enfin – troisième exemple significatif et inquiétant – une machine à café, connectée cette fois, a été la porte d'entrée vers une infection par *ransomware* (à savoir, un logiciel malveillant) dans une usine de production chimique en Europe. Une telle usine, en considération de la dangerosité des produits, était jusqu'alors protégée. Lorsqu'un employé a installé une machine à café intelligente dans le bureau de l'usine, il l'a initialement connectée au réseau local pour lui

---

[266] Loïc DUFLOT*, Contribution à la protection des systèmes d'exploitation et des microprocesseurs* (thèse), Paris XI, 2007.

[267] Steven MEYER, *Les dangers de l'internet des objets* : *ww.bilan.ch/steven-meyer/dangers-de-linternet-choses-iot*

donner accès à l'Internet, ce qui a été en vain. En effet, le réseau isolé n'était pas connecté à l'Internet.

214. Il l'a ensuite connecté au wifi public de la manufacture, mais sans le déconnecter du réseau local. Au bout du compte, l'ensemble des ordinateurs ont été infectés. L'Internet des objets constitue donc une porte d'entrée redoutable pour les attaques et les diverses infestations. Cela tient à plusieurs aspects propres à ces objets. D'une part, ils doivent être innovants et compétitifs. Pour minimiser les coûts et le temps de production, la priorité est donc placée sur le marketing et les éléments vendeurs du produit, comme le *design* ou les diverses fonctionnalités, au détriment de la sécurité. Et ce d'autant plus qu'une cyber-sécurité efficace n'est pas du tout simple à assurer. Elle demande du temps, de l'attention et de l'argent. Or, un seul maillon défectueux suffit. Certaines entreprises sont alors tentées de prétendre faussement que leurs appareils sont sécurisés et protégés, alors qu'ils ne le sont pas.

215. Ces mêmes entreprises achètent quelquefois du matériel – notamment des senseurs – de mauvaise qualité afin de les intégrer à leurs produits. C'est une redoutable erreur. Un matériel vulnérable n'est pas sécurisé. Font également défaut, des mises à jour pourtant indispensables. Cela tient bien entendu à la difficulté de faire les mises à jour d'objets connectés, et au prix fort élevé. Il faut procéder à de nombreux tests. Ce qui est lourd. Une mise à jour mal faite peut avoir des conséquences déplorables : ainsi toute une série de serrures intelligentes fabriquées par une société américaine sont restées bloquées et verrouillées après une mise à jour défectueuse.

216. Certains préfèrent donc conjurer ce risque en les omettant. D'un point de vue technologique, en matière de sécurité des objets connectés, beaucoup de grands efforts restent à faire. Dans l'immédiat, davantage de vigilance permet - sinon d'éviter totalement les risques du moins - de les limiter. Ainsi, il convient d'être attentif. Lors de l'achat d'un produit, il est assez évident qu'une marque reconnue comme Google a plus de chance d'être sécurisée qu'un appareil sans marque ; en provenance d'un pays émergent.

217. Il convient en outre d'être vigilant quant au nombre d'années de mises à jour possibles. Une attention particulière doit également être accordée à la configuration. Les configurations, par défaut, d'un appareil sont rarement les plus sécurisées, hélas. Cependant, le plus grave des problèmes, est que les constructeurs n'ont pas envie de s'investir dans la sécurité de ces objets, pour des raisons d'économie et de temps. Il semblerait donc judicieux de mettre en place des régulations, des normes (De labels de qualité et de certification).

218. Des pénalités sont prévues, souvent lourdes. Ce qui est compréhensible en raison des conséquences. Des labels garantissent la qualité. En considération des risques - en croissance exponentielle - qu'ils posent, les objets connectés devraient faire, eux aussi, l'objet de mesures de réglementation.

Leur essor appelle donc à la fois des cadres juridiques pour sanctionner les abus. De même, des innovations doivent permettre de les éviter en amont, comme le cryptage sophistiqué des données[268].

219. Chiffrer des données implique de les rendre illisibles, grâce à une technique qui doit être la plus sophistiquée possible, sauf si une action spécifique est exercée pour autoriser l'accès. La clé de voûte dans la protection des données repose sur l'ensemble des techniques de chiffrement de données : que l'on appelle aussi techniques de cryptographie.

Ainsi, une donnée ne se présenterait plus de façon claire, mais sous forme cryptogamique. Autrement dit, il faudrait la déchiffrer pour la comprendre. Ce que tout le monde n'est pas, bien entendu, en mesure de faire. Il est nécessaire de disposer d'une clé spécifique qui peut être symétrique (qu'elle permette à la fois pour chiffrer et déchiffrer), ou mieux encore dissymétrique (lorsqu'elle ne sert qu'à l'une des deux tâches).

220. Le chiffrement asymétrique se sert d'une paire de clés mathématiquement liées, dont chacune décrypte le cryptage effectué par l'autre. Ainsi, une seule paire de clés suffit pour permettre à une personne de communiquer avec plusieurs destinataires. Cependant, comme il y a deux clés (une paire), l'une peut rester ignorée alors que l'autre est rendue publique. Ces clés sont plus longues que les clés symétriques. Elles sont donc coûteuses.

221. Bien entendu, la clé de cryptage doit être strictement protégée. Il s'agit de l'objectif le plus important de tous les protocoles de cryptage. Il est certainement essentiel que la clé de cryptage soit soigneusement protégée. L'algorithme de cryptage - lui-même - doit être tenu secret. Concrètement, une telle clé de cryptage se présente comme une suite de caractères aléatoires, souvent divisée en plusieurs parties ou sections.

222. D'une manière générale, plus la clé de cryptage est longue et improbable (se gardant absolument de constituer par exemple une phrase sensée) plus il est difficile de décoder un

[268] Cf. Yehuda LINDELL et Jonathan KATZ*, Introduction to modern cryptography,* Hall/CRC, Maryland, 2014.

message en tâtonnant. Cela est vrai, du reste, du mot de passe que chacun choisit pour protéger son adresse mail.

223. Pour renforcer l'intégrité de cryptage, un procédé courant consiste à demander à plusieurs utilisateurs autorisés de créer chacun leur propre partie de la clé de cryptage complète. Ainsi, le morcellement ne garantit qu'aucun d'eux ne pourra décrypter l'information à lui tout seul. Nous revenons plus loin sur ces défis, dans l'étude systématique de l'enjeu de la criminalité numérique en hausse constante et exponentielle. De façon très concrète, il semble en tout cas - d'ores et déjà - urgent d'inciter fortement, au minimum, les fabricants d'objets connectés à les disposer de systèmes élaborés de sécurité. Des règles et des normes exigeantes devraient être rapidement mises en place. Une politique de sensibilisation aussi bien des producteurs de tels objets que des consommateurs s'impose d'emblée.

224. Outre les dangers liés à la criminalité, il convient de noter celui d'un éclatement chaotique de tous les protocoles. Autrement dit, le caractère problématique de l'Internet des objets ne tient pas seulement au risque d'attaques malveillantes, mais déjà à l'incohérence chaotique que peut susciter l'absence d'un langage commun (induite par la facilité de se connecter sans vérifier les mêmes exigences[269]). De fait, la dynamique même de l'Internet des objets exprime une intention de standardisation de la communication.

225. On peut estimer qu'un système EPC (à savoir, une sorte d'identifiant unique qui permet d'identifier un objet dans une chaîne de production et qui pourrait remplacer l'actuel code-barre[270] en vigueur depuis une cinquantaine d'années pourrait permettre un certain contrôle), constituant une sorte de langage de base soit la garantie d'une identification de chaque objet. Le processus n'est encore que modestement prometteur. En effet, il est payant et à l'état inchoatif. Plus largement, on peut penser que l'Internet des objets peut être conçu comme un cyberespace ouvert, dans lequel des objets autonomes peuvent agir et inter-agir, en vertu d'une intelligence propre.

b. Economie et liberté dans un monde connecté

[269] *Les quatre problèmes de l'Internet des objets : http://alireailleurs.tumblr.com/post/108240810999/les-4-probl%C3%A8mes-de-linternet-des-objets*

[270] Alain MACAIGNE*, La clé du code-barres*, A. Macaigne, Paris, 1989, Claudine SEGALA LABINAL*, Implantation du code-barres,* Toulouse, CNAM, 1994 ; Gaëlle ULMER, *Les problèmes juridiques posés par l'utilisation du code-barres en droit français*, Université de Limoges.

226. D’un point de vue plus directement juridique, l’Internet des objets suppose un renforcement du droit de propriété ; ou, au contraire, selon la philosophie choisie, la mise en place d’une collaboration renforcée et d’un partage des mêmes biens.

On peut, à titre liminaire, mesurer combien un principe aussi simple que « possession vaut titre » semble inapplicable. Il impliquerait des éclaircissements détaillés en vue de son application au domaine des objets connectés

Par ailleurs, en France, la protection des données est une exigence rigoureuse. Son non-respect est lourdement sanctionné. L’article 226-17 du Code pénal le punit de 5 ans d'emprisonnement et de 300 000 € d'amende. Lorsque le coupable est une personne morale - ce qui est le plus souvent le cas en l’espèce, l'amende peut être multipliée par cinq (atteindre 1500000 €).

227. Le manquement au droit au respect de la vie privée n’a rien d’une pure hypothèse abstraite ; qui se vérifierait seulement en cas de régime dictatorial et totalitaire. De plus, elle ne concerne pas seulement les domaines les plus sensibles et les plus délicats. Ceux qui éveillent plus directement la pudeur. L’un des arguments sur lequel s’appuie quelquefois la doxa est le suivant : celui qui n’a rien à se reprocher n’aurait pas à s’inquiéter. Les différentes techniques de surveillance et de contrôle seraient seulement destinées à pister des délinquants ; non à assouvir une curiosité illégitime ; encore moins, à propager des rumeurs.

228. Le raccourci nous semble simpliste, pour deux raisons. D’une part, la transgression du respect de la vie privée nous semble relever du viol d’un droit objectif. D’autre part, elle n’est pas forcément associée à une mauvaise intention en acte. Il serait absurde de culpabiliser celui qui conteste une telle surveillance, comme si cela était la preuve qu’il était coupable de quelque chose.

Ainsi, il faut - en quelque sorte - protéger la vie privée, de façon absolue ; même lorsqu’aucune menace directe ne pèse sur elle. La vie privée doit être protégée des menaces potentielles, même improbables ; non seulement des risques avérés. L’argument consistant, par exemple, à dire qu’un régime en place ne fait peser aucune menace sur les libertés individuelles. Rien ne vaut, en matière de précaution des dérives possibles, pour improbables qu’elles puissent sembler dans la situation actuelle…laquelle situation peut changer très vite. Il suffit donc que la protéction de la vie privée soit potentiellement menacée (même si personne ne s’intéresse aux données éventuellement accessibles) pour que se pose un problème juridique de grande importance.

229. Aux Etats-Unis, le juriste Daniel Solove[271] montre l'étendue et la complexité d'un problème qui se pose avec acuité même dans un contexte d'absence de volonté totalitaire ou de manipulation politique, lors même que les données pour accessibles qu'elles soient ne sont pas disséquées dans les faits, par exemple faute de temps ou de moyens, ou en raison de leur trop grand nombre. Le risque qui pèse sur la vie privée découle déjà d'un déséquilibre entre le consommateur et une entreprise très puissante ; ou entre l'Etat et le citoyen. C'est d'une certaine façon "le pot de terre contre le pot de fer". Il faut donc rétablir un équilibre "perdu", ou du moins compromis. Le contexte se trouve d'emblée grevé d'inégalité Dès lors que notre vie privée n'est plus protégée, il n'y a pas seulement le risque objectif qu'une information secrète puisse être connue, mais encore et surtout de tous les effets de pouvoir qui en découlent. En effet, chacun de nos secrets peut être anodin en soi ou nullement honteux. Il peut constituer une brèche, une fragilité. Il ne faut pas oublier que les recoupements et les associations sont possibles : une seule idée anodine pouvant très bien révéler par déduction (ou induction) des informations plus gênantes. Les autres, à leurs différents niveaux, ont alors du pouvoir sur nous. Il est absurde de croire que nous vivons dans un monde de surveillance généralisée, où l'on épierait nos moindres faits et gestes pour nous piéger. Il serait peu raisonnable de céder à la paranoïa.

230. La théorie du complot fleurit de plus en plus, mais n'a rien de rigoureux. Elle séduit en vertu d'un certain effet Barnum[272] : à savoir, le sentiment d'une coïncidence, comme la promesse vague d'une voyante extra-lucide qui semble correspondre à ce qui s'est passé, ou surtout à nos attentes. Il s'agit alors d'une illusion par défaut de rigueur rationnelle[273], d'une impression prise pour une évidence intellectuelle. Il est - du reste - inquiétant que le développement des nouvelles technologies puisse aussi favoriser la propagation de théories du complot totalement démentes.

231. La diffusion rapide, sinon instantanée des informations, les *fake news* banalisées occultant - en définitive - la notion-même de la vérité, la vitesse avec laquelle tout circule sur le Net sans être

[271] Daniel SOLOVE*, Nothing to Hide : the false Tradeoff between Privacy and Security*, Yale, Yale Press, 2011. A notre sens, un ouvrage capital de référence sur la question.
[272] Serge CICCOTTI, « L'Effet Barnum », *Revue électronique de psychologie sociale*, no 2, 2008, p. 27-31
[273] Sur une critique très juste de développements privés de rigueur scientifique et rationnelle, mais qui font impression et illusion, comme part un exercice de prestidigitation : Raymond BOUDON, *L'idéologie ou L'origine des idées reçues.* Paris, Fayard, 1986 ; *L'art de se persuader, des idées douteuses, fragiles ou fausses*, Paris, Fayard, 1990 ; *Le juste et le vrai : études sur l'objectivité des valeurs et de la connaissance*, Paris, Fayard, 1995. Trois maîtres-livres au crible desquels devraient être soumis bien des propos tenus quelquefois péremptoirement, en particulier sur les ondes ou dans les réseaux sociaux. Seul bémol, Boudon minimise un peu à son époque la force de l'irrationnel dopé par le numérique.

contrôlé (parfois sans que le public-même ait le temps de bien analyser les données) ne peuvent que contribuer à une sorte d'exacerbation des passions et des émotions, peu propice au discernement intellectuel.

232. La passion est souvent fort mauvaise conseillère. Bien entendu, les fausses rumeurs circulent d'autant plus aisément lorsqu'elles sont isolées (non pas insérées dans une sorte de thèse globale). Elles sont également très vite oubliées en raison de la multiplicité - parfois contradictoire - de ce qui est dit ; et de la rapidité avec laquelle ce qui a "fait la une", cesse aussitôt de la faire.

Ainsi, une rumeur isolée fait rapidement place à une autre, tendant à prendre le parti opposé. Les rumeurs peuvent s'agréger en un tout ; constituer une théorie du complot fort séduisante et facilement addictive. Celle-ci flatte notre imagination et revêt alors un semblant de crédibilité.

Elle se présente sous la forme d'un récit théorique d'autant plus convaincant qu'il comble un sentiment de frustration - croissant - face à des nouvelles éparses et difficiles à articuler. Il nous propose une sorte de collier de perles où "tout se tient" : où règne une certaine cohérence, mais fallacieuse. Analysant de façon spécifique les théories du complot comme telles, un sociologue de l'Université de Manchester, Peter Knight[274], les décortique et y discerne une certaine cohérence, fallacieuse, mais susceptible malgré tout de séduire. Elle est facile à diffuser à très large échelle, grâce aux nouvelles technologies. Irréfutable d'apparence, une théorie du complot est dépourvue de scientificité, mais non pas hélas de force de persuasion.

233. Il est, du reste, difficile de discuter avec qui défend une théorie du complot. En effet, toute tentative de la réfuter - ou simplement d'émettre des doutes - sera d'emblée interprétée comme une ruse téléguidée par les conspirateurs eux-mêmes. Au fil du temps, ces discours font courir le risque selon lequel un soupçon pèse sur tout discours rationnel et plus mesuré. Celui-ci étant suspecté d'être un leurre et un mensonge montés de toute pièce par des puissants, tapis dans l'ombre. Toujours est-il que la théorie du complot cherche à adosser à des faits réels un responsable fantasmé ; selon un lien de causalité qui n'est pas démontré, mais qui n'est pas non plus aisément réfutable.

[274] Peter KNIGHT 'Plotting Future Directions in Conspiracy Theory Research', dans le livre de Michael BUTTER et Maurus REINKOWSKI, *Conspiracy Theories in the Middle East and the United States*, Berlin, De Gruyter, 2014.

234. En effet, tout finit par être remodelé pour cadrer avec la théorie fantaisiste. C'est précisément cette difficulté à réfuter une théorie du complot qui la pare d'une crédibilité en réalité fallacieuse. Le philosophe Karl R. Popper [275]avait justement montré que ce qui n'a pas de portée scientifique, paradoxalement, est précisément ce que l'on ne peut réfuter. Le scientifique est le « potentiellement réfutable ».

235. Il est très difficile de mettre en cause un délire avec des arguments rationnels. Ce qui permet à celui qui y adhère et le cultive de le propager de façon plutôt impavide, recueillant donc un certain succès. La question peut se poser, en considération - en particulier - du succès et de l'extension des réseaux sociaux. Souhaitable ou nécessaire de sanctionner du point de vue pénal des *fake news* (surtout lorsqu'elles ont une implication importante, par exemple compromettent des mesures sanitaires urgentes dans le cas du Covid-19), Le phénomène prend chaque jour une importance croissante[276].

236. Il prend de l'ampleur dans nos sociétés traversées par " les autoroutes de l'information" et de la communication, aux vastes ramifications et aux multiples enjeux. Dans ses vœux aux journalistes, du mercredi 3 janvier 2018, le Président Macron estime qu'une législation rigoureuse et précise à cet égard est désormais indispensable en raison de la multiplication de tels phénomènes surtout sur les réseaux sociaux et en général avec une tonalité agressive qui peut aller jusqu'au trouble à l'ordre public.

237. Bien entendu, en Europe, une telle réglementation doit être en conformité avec l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et du citoyen, qui protège la liberté d'expression.

Le droit positif, à l'article 97 du Code électoral, dispose que : « Ceux qui, à l'aide de fausses nouvelles, bruits calomnieux ou autres manœuvres frauduleuses, auront surpris ou détourné des suffrages, déterminé un ou plusieurs électeurs à s'abstenir de voter, seront punis d'un emprisonnement d'un an et d'une amende de 15 000 euros. ». Cependant, ces dispositions s'appliquent à un contexte précis, celui des élections.

---

[275] Karl POPPER, *Conjectures et réfutations, La croissance du savoir scientifique*, Paris, Payot, 1985.

[276] Laurent BIGOT, *Fact-checking vs fake news : vérifier pour mieux informer*, Paris, INA Editions, 2019 ; François-Bernard HUYGHE*, Fake news : la grande peur*, Vapress, 2018 ; Philippe BECHADE, *Fake* News : Post-vérités et autres écrans de fumée, Agora, 2017 ; Florian GOUTHIERE*, Santé, science, doit-on tout gober* ?, Paris, Belin, coll. « Essais », 2017. , 428 p. (ISBN 978-2-410-00930-9).

238. Il convient de préciser que, l'article 27 de la loi du 29 juillet 1881[277]sur la liberté de la presse énonce : « La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros en 1886. Les mêmes faits seront punis de 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation. ».

239. À l'évidence, la rédaction-même de ce texte s'inscrit dans un contexte qui n'est plus celui d'aujourd'hui.

De même, la sanction de *fake news* ne doit pas non plus favoriser la création d'un possible délit d'opinion. Plus récemment, la notion de « fausses nouvelles » semble inclure l'idée d'au moins un fait « précis et circonstancié » (Cour d'appel Paris, 11e chambre, section A, 18 mai 1988) qui n'a pas déjà été révélé (Cassation criminelle 13 avril 1999).

240. La Cour d'appel de Paris précise, dans sa décision du 4 janvier 1998, que : « La nouvelle doit être fausse, c'est-à-dire mensongère, erronée ou inexacte dans la matérialité du fait et dans les circonstances ».

Quant à l'exigence du trouble à l'ordre public : il suffit qu'il soit potentiel. La fausseté peut aussi se manifester par l'exagération - ou la déformation - dans la volonté de tromper. Avec un Internet mondial, le phénomène prend une ampleur jusqu'alors inédite. Sur la toile, les auteurs sont souvent anonymes et les nouvelles vont très vite. Elles "courent", et ne connaissent pas de frontières. C'est donc au niveau international qu'il semble opportun de légiférer.

241. De plus, l'un des critères les plus difficiles à évaluer est celui de la "mauvaise foi". Toujours est-il que, en réponse au souhait du Président Macron, une loi contre la manipulation de l'information a été votée en novembre 2018 - et déclarée constitutionnelle peu après par le Conseil constitutionnel. Elle prend pour cible la diffusion extrêmement rapide des fausses nouvelles sur le Web et les réseaux sociaux. Elle se soucie surtout de la protection des périodes électorales.

Toutefois, le Conseil Constitutionnel a également émis une importante réserve d'interprétation sur la notion de fausse information. Celle-ci ne peut s'appliquer qu'à "des allégations ou

[277] v . Légifrance

imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir". Ces allégations ne recouvrent ni les opinions, ni les parodies, ni les inexactitudes partielles, ou les simples exagérations. Elles sont celles dont il est possible de démontrer la fausseté de manière objective. [...] Seule la diffusion de telles allégations ou imputations répondant à trois conditions cumulatives peut être mise en cause : elle doit être artificielle ou automatisée, massive et délibérée".

242. Un devoir est imposé aux plateformes. Elles doivent mettre en place des mesures pour lutter contre les fausses informations et les dénoncer publiquement. De nouvelles compétences sont confiées au Conseil supérieur de l'audiovisuel (CSA). Il devient le garant du devoir de coopération des plateformes.

    On peut s'interroger sur les limites de cette nouvelle loi, à deux niveaux. D'une part, il n'est pas toujours facile d'évaluer la "fausseté effective" d'une nouvelle. Il y a un risque que cela revienne à une pratique relevant de la censure. Plus largement, on peut émettre de sérieux doutes quant à son efficacité à endiguer un phénomène de très grande ampleur ; qui ne cesse de s'accentuer. L'ingéniosité humaine trouvera de nouvelles parades, si l'on cherche à l'endiguer.

243. La meilleure solution semble être de mener une lutte - en amont - par la sensibilisation et la responsabilisation des jeunes. L'amélioration de la qualité de l'information ne devrait-elle pas surtout passer par des mesures positives - et non répressives. En vue de la mise en place d'un véritable service publique d'information qui coupe l'herbe sous les pieds des faux annonceurs ? Pour Divina Frau Meigs, chercheure en Sciences de l'information et membre du groupe d'experts sur les *fake news* de l'Union européenne, la loi ne suffira pas à bloquer le phénomène. La solution durable et soutenable à la lutte contre la "*mal information*" passe par l'éducation des jeunes et des moins jeunes à un usage responsable des médias de masse et des médias sociaux.

244. L'éducation aux médias et à l'information (EMI), en transmettant la maîtrise des codes, des langages et des pratiques médiatiques et numériques, est le meilleur moyen pour apprendre à distinguer l'information de qualité ; et repérer les fake news

    La lutte contre les fausses informations - pour la qualité de l'information - passe par des mesures propres à limiter : l'influence des annonceurs, la concentration de la propriété des médias et la précarisation du statut des journalistes. Ainsi, selon le collectif Action-critique-médias

(Acrimed) le texte est trop centré sur les fausses informations sur l'Internet, alors que la lutte "contre les pires dérives" (et l'amélioration de la qualité de l'information) devrait passer par la "construction d'un véritable service public de l'information et de la culture, la création d'un statut de média à but non lucratif, d'un statut juridique des rédactions, ou encore la garantie de l'indépendance des sociétés de rédacteurs".

245. Cette loi peut en tout cas être jugée "liberticide". Elle a suscité de vives critiques, comme celles de l'écrivain et juriste François Sureau qui doivent inciter à la vigilance d'autres pays lorsqu'ils amenderont leur droit positif.

Une telle loi semble renforcer un climat général plutôt délétère. Elle peut donner l'impression « d'un pays où les libertés ne sont plus un droit mais une concession de pouvoir, une faculté susceptible d'être réduite, restreinte, contrôlée autant dans sa nature que dans son étendue »[278].

246. D'autre part, avec beaucoup de finesse, le même François Sureau estime "malheureux" et d'ailleurs "contre-productif" de confier au juge des référés - qui doit évaluer le caractère fallacieux ou non d'une information - une capacité de discernement. Celle-ci revient aux citoyens : « Là encore Gribouille a eu le dernier mot. Le juge des référés peut donc être saisi de la fausse nouvelle, de crainte que le citoyen, décidément réputé stupide par ses dirigeants en dehors bien sûr des moments où il les choisit, ne puisse peser par lui-même la valeur de la nouvelle en cause. Mais le juge des référés est celui de l'évidence. Dans la généralité des cas, il lui sera impossible de démêler le vrai du faux. Les requêtes seront donc le plus souvent rejetées, comme il est habituel. Le public sera fondé à penser que la fausse nouvelle est vraie, ce qu'il n'aurait pas nécessairement fait en l'absence d'un tel dispositif »[279].

247. Une loi récente s'inscrit "dans la même lancée". Elle a également fait couler beaucoup d'encre, avant d'être censurée par le Conseil Constitutionnel. Il s'agit de la loi contre les contenus haineux sur l'Internet (dite « loi Avia » du nom de la rapporteuse, Laetitia Avia).

Ainsi, elle prévoit une série de mesures visant à nettoyer des contenus terroristes et pédopornographiques qui circulent sur l'Internet - le plus vite possible. Le texte est adopté une

[278] François SUREAU, *Sans la liberté*, Paris, Tracts Gallimard, n° 8, 2020, 21.
[279] *Ibid*., 21-22.

première fois par l'Assemblée nationale le 9 juillet 2019 ; puis, par le Sénat le 17 décembre 2019 ; avant d'être adopté de façon définitive au Palais-Bourbon le 13 mai 2020. Cette loi suscite - d'emblée - beaucoup de critiques et de réserves. D'aucuns y voient une nouvelle limitation des libertés individuelles ; en particulier de la liberté d'expression.

248. Etienne Gernelle dans son édito de l'hebdomadaire « Le Point » du 21 mai 2020 s'exprime en ces termes : « La loi Avia s'ajoute à plusieurs pulsions orwelliennes récentes, comme la loi dit « anti-fake news » qui prévoit elle aussi un renforcement des pouvoirs du CSA. Dans un registre plus folklorique, elle prolonge également les tentatives d'établir un pseudo-conseil dit de « déontologie » de la presse, sous le patronage insistant du pouvoir, et la création d'un portail d'information – vite disparu – recensant les articles sur le Covid-19 que le gouvernement jugeait conformes. L'exécutif a-t-il un problème avec la liberté d'expression ? »[280]

249. Le manque de précision juridique et de réelle pertinence se retourne donc toujours contre le législateur, et contre le bien commun. Non seulement l'effet recherché n'est pas atteint, mais c'est l'inverse qui finit par advenir. La censure exercée par le Conseil Constitutionnel constitue à cet égard un événement important et lourd d'incidences - sans doute - pour le futur.

    En effet, l'éminente institution redoute que les plateformes, par crainte de sanctions démesurées, n'en viennent à « sur-censurer ». Ceci, d'autant plus que le délai laissé pour le discernement ne doit pas être trop bref; sauf à vouloir produire un effet de panique.

    Comme le rappelle justement l'avocat Jean-Sébastien Mariez: « La décision rappelle le rôle essentiel du juge pour qualifier et apprécier les contenus en ligne ». Il semble que toute notre attention doive être portée sur les critères de définition de la notion de haine. Même si le phénomène de l'exacerbation des passions, en particulier sur l'Internet, est inquiétant : " Comment tracer une délimitation précise entre une polémique un peu virulente, parfois au second degré, et des attaques haineuses ? "

250. Le débat s'avère également complexe dans la mesure où l'on peut se demander si le défouloir de haine (qui s'étale, par exemple, sur Facebook) favorise une déstabilisation sociale. Fait-il peser une menace, ou au contraire, constitue-t-il un processus de *catharsis*, susceptible de libérer de doutes - d'apaiser ?

[280] *Le Point*, 2491, 21 mai 2020, 6.

251. La question est délicate à trancher. Il se peut que les deux hypothèses soient vraies ; dans des proportions à déterminer, selon les contextes, et surtout les individus. Le propos haineux est - en soi - différent d'une mauvaise information ; même si un même propos peut rentrer dans les deux catégories à la fois. Il n'est déjà pas simple d'appliquer un critère de véracité d'une allégation ; encore moins de déterminer si elle a été prononcée avec l'intention de nuire, ou de mauvaise foi.

252. La notion de haine ne semble tout simplement pas pertinente en droit. Elle ne figure pas directement dans le droit positif français. Toutefois, on peut la retrouver, de façon détournée, dans la sanction de "l'incitation à la haine" que punit la loi René Pleven de 1972[281]

253. D'ailleurs, l'idée de " couper l'herbe sous les pieds" à toute rhétorique haineuse remonte à la fin des années 1930. À une période où l'on a assisté à la montée du nazisme et des fascismes, A vrai dire, hélas, la France a toujours connu des déferlantes de propos haineux, par exemple antisémitises. On peut citer la « France juive », le tristement célèbre pamphlet d'Edouard Drumont (en pleine affaire Dreyfus)[282].

    Cependant, les ordinateurs, téléphones et Ipads semblent favoriser un passage à l'acte dans l'expression, que ne permettaient pas le courrier ou la presse écrite. Souvent de façon compulsive, des pensées peu amène et peu bienveillantes – c'est une litote – déferlent sur Facebook

254. En 1939, dans un contexte singulièrement tendu, le ministre de la justice Paul Marchandeau édicte un décret-loi assez sévère (en date du 21 avril) par lequel il décide que la diffamation ou l'injure seraient désormais sanctionnées ; de façon systématique ; y compris, en l'absence d'une plainte des personnes ou des groupes concernés. Les propos poursuivis visent des personnes pour leur origine, leur race ou une religion déterminée.

255. Ainsi, la loi Avia a créé une forte tension. Ceci, dans la mesure où les sites doivent retirer les propos jugés inadmissibles dans un délai de 24h. Ce qui est - à l'évidence - un délai très court. Le retard pourra être lourdement sanctionné. Des questions se posent quant à savoir si et

[281] v. en ligne
[282] Michel WINOCK, *Édouard Drumont et Cie. Antisémitisme et fascisme en France,* Paris, Seuil, 1982,

comment les mesures prévues par la loi seront applicables. En effet, elles supposent que l'on mette les moyens. De même, la crainte d'un retour de la censure grandit aujourd'hui. Ce qui explique la saisine du Conseil constitutionnel français par plus de soixante sénateurs. *TECH IN* France, l'un des principaux syndicats de l'industrie du numérique partage ces inquiétudes

256. Dans la revue « Contrepoints », Yannick Chatelain, auteur de nombreux ouvrages sur le digital numérique, dénonces-en des termes très forts cette loi qui pousse au plus haut le curseur de censure automatisée. De même, dans son excellent pamphlet déjà cité François Sureau, nous met en garde contre une dérive liberticide. Selon lui, elle finit par devenir indolore. Elle ne peut qu'altérer nos principes démocratiques. Il y a un abus à vouloir s'en prendre à la haine, qui relève du for interne (et donc en principe ne tombe pas sous les décisions discrétionnaires des lois et des juges) : « En se fondant sur la notion de haine qui est un sentiment relevant du for intérieur, la loi introduit désormais la répression pénale à l'intérieur de la conscience. Cette République dont tous nos partis se réclament c'est bien pourtant « la haine des tyrans » qui l'a soutenue dans ses débuts. La haine peut être blâmable – elle ne l'est pas toujours. Elle ne peut, à elle seule, représenter une occasion de condamner. Comme en matière de terrorisme, cette idée simple que penser n'est pas agir, que dire n'est pas faire qu'avant l'acte criminel il n'y a rien, là cède chaque fois davantage aux nécessités d'un contrôle social de plus en plus rigoureux (…) Ce texte constitue donc un puissant encouragement à la censure, puisque les opérateurs privés des grands réseaux d'informations préféreront, dans le doute, censurer une expression plutôt que de voir leur responsabilité mise en cause »[283].

257. On ne peut aisément dissiper le sentiment de perplexité qui tient au fait que le texte confie précisément aux fâmeuses GAFAM (Google, Amazon, Facebook et Apple) le soin de réguler une liberté publique ; le soin de censurer, avec un risque de surveillance générale exercé par ces dernières. Ils exerceraient une censure arbitraire. Ils s'arrogeraient alors un pouvoir qui n'est pas de leur compétence. Certains esprits chagrins sont tentés de rapprocher la loi Avia de lois controversées promulguées en Russie par le Président Poutine ; jugées, elles aussi, liberticides. Il s'agit de deux lois promues le 18 mars 2019 La première d'entre elle s'en prend aux fausses informations socialement significatives et présentées comme si elles étaient vraies. En l'occurrence les fameuses fake news.

[283] François SUREAU, *op. cit*, 22-23.

258. La seconde, pour sa part, criminalise les offenses aux symboles de l'Etat et à ceux qui le représentent. À l'évidence, il s'agit de couper "l'herbe sous les pieds" à toute critique du pouvoir. Le contexte français n'est pas le contexte russe.

Toutefois, une certaine similitude d'intention et de contenu, toute proportion gardée, pourrait inciter à la vigilance. La mise au point d'un algorithme, qui serait un crible particulièrement rigoureux, ferait peser une très grave menace sur les libertés. En France, il faut savoir que plus de 400 lois et articles des Codes pénal et civil nuancent - sinon limitent - les principes posés par la Déclaration des droits de l'Homme et du Citoyen de 1789, pour tout ce qui concerne la liberté d'expression.

259. Placer le curseur à l'endroit exact qui serait un point d'équilibre entre la préservation de la liberté d'expression et la protection contre d'autres menaces n'est pas simple. Une dérive dans un sens ou l'autre est toujours à redouter. Cette considération peut aussi être utile à d'autres pays, qui sont en cours d'élaboration des lois ou règlements en la matière.

260. Sur le rôle dangereux que pourraient jouer alors les GAFAM, il y aurait encore beaucoup à écrire[284]. A l'évidence, ces géants des nouvelles technologies peuvent-ils se servir des informations personnelles fournies gratuitement par les utilisateurs pour dresser des profils détaillés de chaque utilisateur ? En particulier, dans le but de leur adresser des propositions bien ciblées grâce à l'intelligence artificielle qu'ils utilisent.

Se créer, ainsi, une base de données largement interconnectée ; susceptible d'être revendue à des publicitaires - très heureux de pouvoir ainsi mieux choisir leurs cibles. De même, ces profil peuvent être vendus à des gouvernements étrangers (pour les associer aux techniques de reconnaissance faciale et à d'autres outils de surveillance). On peut aussi, dans des cas plus extrêmes, relier les profils personnels ainsi composés avec des informations volées -via le piratage de dossiers administratifs de certains Etats)

261. Il faut encore souligner le coût social dissimulé de ces géants dont le consommateur pourrait être la victime sinon – que l'on nous pardonne l'expression – le « pigeon ». C'est un article de

[284] Nikos SMYRNAIOS*, Les GAFAM contre l'internet*, Paris, éditions Ina, 2017 ; Jacques FONTANEL et Natalia SUSHCHEVA, *La puissance des GAFAM : réalités, apports et dangers*, Paris, La Documentation française, 2019.

presse paru dans *le New York Times* du 13 juillet 2019 qui s'exprime en ces termes : « Des dizaines de bases de données contenant les visages d'individus ont été compilées sans qu'ils le sachent par des sociétés et des chercheurs. Un grand nombre de ces photos étant ensuite partagées dans le monde entier, au sein de ce qui est devenu un vaste écosystème alimentant la propagation de la technologie de reconnaissance faciale. Les bases de données sont constituées à partir de photos provenant des réseaux sociaux, de sites de photos, de sites de rencontre comme OkCupid et de caméras disposées dans des restaurants et sur des sites universitaires »

262. Cette entrée violente dans la vie privée, suite à la collecte de photos de visages, devrait être traitée avec la plus grande sévérité. Une rumeur prétend que Google serait infiltré par les services de renseignement chinois ; après avoir refusé de travailler avec les services de renseignements américains

    Le gouvernement américain cultive le soupçon à propos d'une possible duplicité de Google Facebook aurait également l'intention de créer une cryptomonnaie du nom de *libra*, d'où son rejet du Bitcoin, en fait pour le concurrencer Ce géant technologique semble donc se conduire comme un état souverain créant sa propre monnaie.

263. Une opposition assez unanime des gouvernements, des parlements, des médias et bien entendu des banques centrales semble exister…pour le moment. Il faut savoir que le *libra* fonctionne ainsi comme une banque Toutefois, sans l'agrément qui va avec. Ce serait évidemment dissuasif pour Facebook. Le projet *libera* n'est donc pas près de se réaliser - encore que tout peut s'accélérer. Cependant, il est révélateur de l'ambition démesurée de Facebook.

264. Partout dans le monde, devrait se multiplier les lois contre les géants de la technologie et aussi des actions en justice. Cette multiplication, au-delà d'un certain bien-fondé moral ou juridique éventuel pourrait poser un problème de sécurité juridique (associé à toutes les phases de transition associées au progrès technique). Des coûts peuvent en résulter. Ils peuvent être des frais d'autorisation facturés par des consommateurs ou encore une perte de revenus émanant de gouvernements étrangers.

    Toutefois, à long terme, ces processus de contrôle pourraient profiter par un effet de compensation aux actionnaires eux-mêmes qu'il faudrait en quelque sorte dédommager des risques pris. Dans la perspective actuelle d'incertitude quant à la règlementation, les divers investisseurs affinent leur stratégie. Une certaine méfiance règne concernant Google, Amazon

et Facebook. Les interventions éventuelles des gouvernements les concernant pourraient être fort perturbantes pour leurs activités et les pénaliser financièrement.

265. Ainsi, à court terme, pénaliser les différents actionnaires. Mais à moyen et long terme, une fois la perspective clarifiée, la situation des actionnaires pourrait s'en trouver au contraire améliorée. Par exemple, il pourrait être alors possible d'acheter des actions bon marché. Et les investisseurs pourraient même récupérer gratuitement des actions d'entreprises solides dont les géants de la technologie auraient dû se séparer.

Ainsi, sans aucun doute, la société et toutes ses composantes dans leur diversité, peuvent nous opprimer et nous manipuler avec beaucoup de facilité. C'est cela qui est scandaleux d'un point de vue éthique. Même la connaissance de données peu intimes ou compromettantes peut constituer une arme pour celui qui la contrôle car elle permet de « tenir » d'une certaine façon ceux qui l'ont eu. Le problème ne réside pas tant dans la surveillance-même des données, mais dans l'impuissance et la vulnérabilité créée par une utilisation de données qui exclut la personne concernée (de la connaissance ou de la participation à un processus qui la concerne).

266. Le citoyen risque ainsi de devenir un pion entre les mains de bureaucraties elles-mêmes aveugles du reste, et fonctionnant parfois de façon chaotique, ou concurrentielle, sinon contradictoire. C'est l'ensemble du fonctionnement social qui risque alors de devenir aliénant. La confiance entre les individus et à l'égard de l'Etat risque ainsi d'être menacée.

267. Le risque n'est nullement illusoire. On peut penser aux avatars tragi-comiques vécus par un des candidats à la mairie de Paris en 2020, Benjamin Griveaux, très vite oubliés et recouverts - il est vrai - par la surmédiatisation de la menace que fait peser comme une épée de Damoclès inattendue le Covid-19.

268. Candidat d'un parti important à la mairie de Paris, M. Griveaux se retire lui-même de la course. Ce à quoi il n'était - du reste - pas contraint d'un point de vue juridique ; suite à la diffusion d'une vidéo à caractère sexuel, dont il serait l'auteur bien imprudent et qu'il aurait envoyée à une femme avec laquelle il échange. Cette vidéo a été volontairement postée en ligne par l'artiste Piotr Pavlenski, dans le but de tourner en dérision la classe politique et ses représentants. Ce militant entendait dénoncer l'hypocrisie d'un candidat qui se réfère aux valeurs morales et à la famille (tout en menant une vie personnelle aux antipodes des idéaux affichés) Ce qui, soulignons-le, est par ailleurs tout à fait son droit dans une société comme la

nôtre qui ne sanctionne pas d'un point de vue juridique et pénal des mœurs que d'aucuns peuvent trouver dissolues, sous certaines réserves bien entendu.

269. Il ne fait aucun doute, cependant, qu'un tel écart entre ce qui est dit et la pratique réelle, ne relevant certes pas du pénal sont pourtant susceptibles de troubler fortement l'électorat potentiel du candidat concerné. Même si cette vidéo à caractère pornographique est filmée dans le cadre d'une relation consentante entre deux personnes majeures. Il est bien entendu essentiel de souligner que Benjamin Griveaux a porté plainte pour atteinte à sa vie privée. Si c'est bien lui qui a filmé la vidéo pour son usage tout personnel, il n'entendait aucunement qu'elle puisse être rendue publique en raison précisément de son caractère très intime. C'est sa partenaire qui aurait communiqué à un tiers cette vidéo. Celui-ci s'empressant alors de la diffuser mais sans l'accord de l'intéressé.

270. Il y a quelques années déjà un élu parisien a été mis en difficulté lorsque le magazine Têtu avait rappelé - assez méchamment - qu'il avait tourné dans un film porno oublié, mais qui relève du domaine public. Du point de vue pénal, il y a bien entendu une forte dissymétrie entre les deux situations. Pourtant, dans les faits, il s'agit d'une même volonté de nuire, voire de détruire psychologiquement, avec des conséquences qui peuvent s'avérer très graves.

271. Du point de vue de la loi française, la publication en ligne d'images intimes est sévèrement punie par la loi française. Une loi de 2016 prévoit une peine de deux ans de prison et 60 000 euros d'amende pour la diffusion de ce type d'enregistrement. La sanction se présente comme bien plus sévère que pour les atteintes à la vie privée qui ne présentent pas de caractère sexuel. Du reste, en théorie, elle peut s'étendre à toutes les personnes ayant contribué d'une façon ou d'une autre à la diffusion des vidéos, même si - dans les faits - la justice s'attaque surtout aux personnes qui ont initialement mis le fichier en ligne. Poursuivre l'ensemble des personnes ayant diffusé des liens vers le site serait impossible et sans doute ridicule.

272. Nous avons précisé ce qu'il faut, en définitive, penser des théories complotistes et de ce qu'elles affirment. Nous nous sommes également interrogés sur la question de savoir s'il faut - et comment - sanctionner ceux qui les propagent avec le risque de menacer la liberté d'expression. Il n'est cependant nullement interdit de s'interroger également sur des dérives potentielles graves que peut faire peser l'introduction d'une application comme " Stopcovid ". En effet, dans la perspective de lutter contre la propagation de la pandémie, le gouvernement français a travaillé sur une petite prouesse technologique : à savoir une application de suivi des personnes

positives au Covid-19 par le "suivi de ses contacts" (ou "*contact tracking*"), afin d'avertir celles qui sont entrées en contact avec elles, via leur téléphone portable.

273. Au-delà des difficultés techniques évidentes d'un tel projet, d'autant plus qu'il s'agit de le mettre au point très rapidement, se posèrent également de redoutables questions éthiques et juridiques. La vigilance s'impose face à toute dérive possible. Lors même que le but recherché n'est évidemment pas un contrôle insupportable des populations - excessivement restrictif des libertés, cela pourrait pourrait être une conséquence inquiétante, échappant à la bonne volonté initiale : à la prudence de ceux qui sont à l'origine d'un tel projet.

274. L'enjeu est évidemment important : il s'agit de briser les chaînes de transmission du virus. Cela peut éviter d'avoir recours à des mesures plus extrêmes (comme un confinement) avec des corollaires économiques très graves et des conséquences humaines, psychologiques, non négligeables. L'application *Stop Covid*, destinée aux smartphones, est développée dans le but très légitime de répertorier les personnes testées positives au Covid-19 et d'avertir celles qui sont entrées en contact avec elles, via leur téléphone portable. Son utilité semble indiscutable. Pour que cette application puisse être efficace, il faut cependant que la personne testée - positive au virus - se déclare. Elle doit accepter - en quelque sorte - de "jouer le jeu" : à savoir, que les autres utilisateurs puissent avoir accès à cette information la concernant.

275. L'anonymat semble respecté dans le cadre strict des diverses conditions établies par les directives européennes en vigueur : le RGPD Règlement général sur la Protection des données L'utilisation d'une telle application se fait uniquement sur la base du volontariat, et d'un volontariat éclairé sur sa nature, sur les données utilisées, le temps de conservation et les modalités d'effacement

    En aucun cas, une quelconque liste nominative de personnes contaminées, avec un risque évident de stigmatisation, ne saurait constituée, avec un risque évident de stigmatisation sociale

    Toutefois, il ne s'agit pas simplement de données statistiques de nature globale, comme celles recueillies par exemple au début de la pandémie par Orange en France permettant de voir qu'un très grand nombre d'abonnés se trouvent dans une zone, laquelle zone présente donc un fort risque de contagion.

276. Dans un tel cas, aucun des abonnés ne peut être identifié d'aucune façon. Il s'agit simplement d'un constat statistique. Malgré la prudence avec laquelle l'application est conçue, des risques semblent devoir être considérés. Ce qui explique peut-être pourquoi un nombre limité de personnes seulement a initialement téléchargé et utilisé l'application en France (environ 2 ou 3

millions). Si le principe du volontariat ne semble pas être mis en question, de façon plus subtile, des pressions peuvent s'exercer (par exemple, de culpabilisation de celui qui refuse une telle application). Ce qui demeure toujours son droit, certes, mais peut le faire soupçonner d'incivisme. En aucun cas, l'utilisation effective de l'application ne saurait être posée comme une quelconque condition pour des soins, pour des tests, ou pour l'accès à des transports en commun. Les personnes ayant l'application doivent garder leur téléphone allumé. Ce qui est une contrainte.

277. Les risques de détournement des données ou d'usage pervers, même non intentionnel au départ, impliquent donc qu'une telle application ne soit mise en place qu'à la condition expresse de sa véritable utilité et dans le cadre d'une politique globale et harmonisée de lutte contre la pandémie.

    Telle est en France la position adoptée par la CNIL. L'utilisation de cette application doit évidemment être temporaire et faire l'objet d'une évaluation fréquente, quant à son utilité effective. Il serait en revanche judicieux, par la suite, que le recours à de semblables dispositifs de contrôle soit très rigoureusement encadré, par un fondement juridique explicite dans le droit national. On peut cependant estimer que la CNIL n'est pas assez prudente et limitative face à un dispositif centralisé qui ne présente pas de garantie suffisante. Le risque semble réel d'une accoutumance dangereuse à une surveillance généralisée.

278. L'enjeu est philosophique : jusqu'où peut-on limiter la liberté ou lui faire courir de graves risques pour la sécurité ?[285] Il y a peut-être une position médiane à trouver. D'un point de vue concret (et dans l'urgence) ce n'est pas simple. Or, il s'avère - depuis - que l'application récolte plus de données que ce qui avait été annoncé par le gouvernement. Le Secrétaire d'Etat chargé du Numérique, Cédric O, comme l'établit le chercheur en cryptographie Gaëtan Leurent, souligne que tous les contacts croisés pendant quatorze jours ont été envoyés par l'application au serveur central, hébergeant les données, contrairement à ce qu'avait annoncé le gouvernement (qui avait assuré que seuls les identifiants des téléphones des utilisateurs ayant été en contact pendant 15 minutes à moins d'un mètre de distance d'une personne testée positive au Coronavirus seraient conservés).

[285] Le philosophe français André Comte-Sponville, ancien membre du Comité consultatif national d'éthique : « Pas question, sur le long terme, de sacrifier la liberté à la santé. J'aime mieux attraper le Covid-19 dans un pays libre qu'y échapper dans un État totalitaire! » *(https://www.lecho.be/dossiers/coronavirus/andre-comte-sponville-j-aime-mieux-attraper-le-covid-19-dans-un-pays-libre-qu-y-echapper-dans-un-etat-totalitaire/10221597.html.*)

279. Selon Gaëtan Leurent, "*StopCovid*" envoie donc une grande quantité de données au serveur qui n'a pas d'intérêt pour tracer la propagation du virus, mais qui pose un vrai danger pour la vie privée". Et il ajoute : "j'ai fait un test en installant "*StopCovid*" sur deux téléphones, et en l'activant une dizaine de secondes avec les deux téléphones dans deux pièces différentes (environ 5 mètres de distance, plus un mur). Quand je me déclare ensuite comme malade, mon appli envoie bien ce contact sur le serveur, alors qu'il n'a aucun intérêt épidémiologique."[286].

280. Par-delà un contexte particulièrement complexe, au fil de son analyse, Daniel J. Solove, recense diverses séries de problèmes (sur lesquels il nous faudra revenir un peu plus tard) qui ont beaucoup en commun.

L'enjeu fondamental, d'un point de vue juridique, est le maintien d'une véritable démocratie sur fond d'inégalité des forces initiales. Ce que Solove veut nous dire, en définitive, c'est que le bras de fer ne peut pas être égal entre le simple citoyen - d'une part, et des groupes puissants ou des Etats - de l'autre.

281. Lorsque la vie privée du simple citoyen n'est plus protégée, il se trouve facilement sous la coupe d'adversaires beaucoup plus puissants à cause des moyens considérables - de toutes natures - dont il dispose. La vulnérabilité qui le menace peut-être lourde de conséquences. C'est la raison pour laquelle, il est si important de prévenir toute atteinte possible au droit de protéger sa propre vie privée ; même lorsqu'il s'agit de choses anodines[287].

282. Il est absurde et dangereux pour Solove de vouloir relativiser ce droit, en confondant purement et simplement la vie privée, avec des choses inavouables à cacher soigneusement : la vie privée inclut aussi toutes les données personnelles que rien ne doit obliger de communiquer aux autres[288]. Or, la surveillance par les données constitue aujourd'hui une dérive potentielle et - en partie déjà réelle et - très périlleuse.

---

[286] *https://www.sortiraparis.com/actualites/a-paris/articles/221583-coronavirus-l-application-stopcovid-recolte-plus-de-donnees-qu-annonce*

[287] Cf. l'exemple français : Basile ADER, « La protection de la vie privée en droit positif français » : *https://www.cairn.info/revue-legicom-1999-4-page-5.htm*

[288] Bénédicte REY, *La vie privée à l'ère du numérique*, Paris, Sciences Pub, Lavoisier, 2012 ; Fabrice ROCHELANDET, *Economie des données personnelles et de la vie privée*, Paris, Ed. La Découverte, Collection Repères, 2010.

283. La « *dataveillance* », comme l'appelle Roger Clarke[289], consiste en une réutilisation systématique de systèmes de données personnelles pour enquêter (ou surveiller les gens). Cette réutilisation semble - hélas - de plus en plus aisée. Le plus agaçant - mais aussi inquiétant - est que nous ne savons pas exactement de quelles façons nos données sont connues, fouillées et explorées.

284. L'ignorance du plus grand nombre est - à certains égards - plus abyssale que jamais, en considération des enjeux. La surveillance - même potentielle - par les données pose un problème structurel. Elle est révélatrice de la façon dont les gens sont traités par les personnalités morales telles que les institutions et les grands groupes, par exemple.

Au-delà du contrôle systématique - qui passe plus difficilement inaperçu, il faut signaler l'addition de petites données recueillies un peu partout. Celles-ci, comme une foule d'indices, peuvent devenir d'autant plus concluantes. Le croisement des données permet d'acquérir les connaissances les plus précises et déjouer les pièges. En effet, des entreprises et de grands groupes peuvent habilement respecter à la lettre le consentement du consommateur, mais contourner - en quelque sorte - les barrières de protection, en croisant différentes données. Violer frontalement certaines normes serait sans doute trop coûteux et trop dangereux pour eux. En revanche, il y a moyen de parvenir à des connaissances aiguisées par un croisement judicieux, en quelque sorte latéral. Il pourrait apparaître comme inattaquable ; dans la mesure où aucune donnée confidentielle n'a été quant à elle divulguée. La possibilité de contournement des lois semble vraiment considérable.

285. De nos jours, ce ne sont plus tant les données personnelles - prises individuellement - qui ont de la valeur que le croisement de plusieurs de ces informations. Un consentement donné à deux entreprises quelconques de revente des données personnelles leur permet d'échanger et de connaître beaucoup de choses. Le croisement est toujours beaucoup plus fécond en informations nouvelles qu'une simple récolte de données brutes, dans la mesure où certaines de ces dernières pourraient s'avérer imprécises ou fausses. Le statut du résultat obtenu par le croisement est alors plus ambigu et plus difficile à déterminer.

286. En effet, même en donnant à deux entreprises le droit de revendre des données personnelles, cela autorise-t-il vraiment les deux entreprises à revendre ce qui n'est pas la simple addition brute de données, mais le croisement (offrant un surcroît informatif), lui aussi personnel ? Nous ne sommes pas dans la perspective d'une simple collecte de données que l'on pourrait revendre

[289] Cf. son site personnel : Roger CLARKE*, http://www.rogerclarke.com/DV/*

à d'autres, mais dans une sorte de création de nouvelles données à partir du croisement de données. Ce qui constitue un problème juridique *sui generis*, et très délicat.

287. Cette super-donnée est obtenue par croisement. Celui dont les données ont été croisées ne la connaît même pas ! Il faudrait lui en donner non seulement connaissance, mais également la pleine propriété. En reconnaissant qu'elle lui appartient. Cela impliquerait alors de faire de la donnée un élément relevant de la propriété. Ce qui semble en totale contradiction avec notre droit. Une donnée personnelle[290], en effet, est une donnée qui se rapporte strictement à un individu et permet de l'identifier. Elles relèvent globalement de ce que les anglais appellent « privacy » ; de la " sphère privée ". Les délimitations de cette notion sont bien entendu subtiles.

288. Les aspects économiques et financiers sont - de plus en plus ciblés. Ils visent à adapter une stratégie marketing au plus près des besoins du client. Les données personnelles se présentent comme des marchés. Elles sont devenues un enjeu prioritaire. Une donnée devient - de plus en plus - une réalité aux contours flous et élastiques. Elle contient, d'une part, "l'information brute", mais également " son interprétation" ; par exemple, de l'âge, ou de l'orientation sexuelle, tel type de centre d'intérêt commercial. Nous reviendrons - plus loin - sur l'idée d'accorder, par voie de patrimonialisation, un autre statut à une donnée (pour mieux la protéger).

289. L'Europe, surtout latine, de façon assez ancienne, respecte la spécificité de la sphère privée. Cela se retrouve dans son droit. Ce qui ne semble pas être le cas aux Etats Unis.

Il est vrai que la frontière tracée entre le privé et le public ne semble pas être la même. Cela est également vrai des actions morales, touchant notamment à la sexualité (plus sévèrement réprimées aux Etats Unis, ou en Angleterre ; comme l'atteste la célèbre affaire Oscar Wilde à la fin du XIXe siècle[291]). Dans la mentalité plus européenne, les secrets privés de chacun doivent être soigneusement protégés, non seulement contre les visées prédatrices, mais aussi la simple indiscrétion, voire les velléités de contrôle de l'Etat.

290. Or, la révolution numérique est en bonne part américaine. Ainsi, il n'existe pas d'emblée une sorte de culture juridique ou éthique inhérente à l'inflation des données, afin de protéger la vie privée. Il faut plutôt tenter de mettre en place des garde-fou en les ajustant à une réalité née, au

[290] Guillaume DESGENS-PASANAU, *La Protection des données à caractère personnel*, Paris, Litec LexisNexis, collection Carré Droit, 2012,

[291] Odon VALLET, *L'affaire Oscar Wilde ou du danger de laisser la justice mettre le nez dans nos draps,* Paris, Albin Michel, 2014.

départ, dans un autre contexte même s'il s'internationalise. Des pratiques " courantes " aux Etats Unis sont considérées comme "choquantes" en Europe, car portant atteinte à la dignité de la personne et donc à la liberté individuelle.

Or, les données ont - aujourd'hui - une dimension internationale ; plus seulement anglo-saxonne. Ce qui suppose de reconsidérer l'aspect juridique de la question ; sans méconnaître pourtant la diversité de mentalités et de points de vue. En effet, la mentalité étasunienne a tendance à considérer la donnée personnelle comme n'importe quelle information. Ceci, d'autant plus qu'elle est marquée par une exécration du mensonge. Cette mentalité s'est manifestée et a surpris les Européens, notamment au moment de l'affaire Clinton[292].

291. Elle est plus sensible au mensonge qu'à la légitimité éventuelle pour une personne de vouloir maintenir secrète (ou discrète) certaines dimensions de son existence. La mentalité européenne est beaucoup plus soucieuse du respect de la confidentialité et de la dignité de la personne.

De nombreuses questions ne manquent pas alors de se poser : " Faut-il envisager un compromis entre ces deux mentalités ? Et dans quelle mesure ? Dans quelles proportions ? Faut-il accepter une coexistence - selon les espaces géographiques - de pratiques différentes ?" Ce qui devient de plus en plus problématique dans un monde aussi unifié que le nôtre.

292. " À l'ère de la mondialisation, n'est-il pas absolument impératif de prévoir une réglementation à l'échelle planétaire ? " Derrière le questionnement philosophique et juridique se dissimulent, sans aucun doute, des enjeux sociétaux considérables. C'est ainsi que se pose un redoutable problème. La législation française se veut claire et rigoureuse, et à certains égards se présente comme un modèle. L'une des raisons de cette sensibilité française particulière tient à l'histoire, et en particulier au gouvernement de Vichy. Ce dernier, en effet, pendant la Seconde Guerre Mondiale, avait fiché les Français, en fonction de leur race et de leur origine. En 1974, la mise sur pied du projet "Safari" (de croisement des données nominatives) a suscité un mouvement d'inquiétude et une mobilisation des consciences.

293. C'est pourquoi, a été votée le 6 janvier 1978 une loi de garantie de la liberté et de la confidentialité, relative à l'informatique, aux fichiers et aux libertés, loi dite "Informatique et Libertés ". Elle précise que l'informatique doit être exclusivement placée au service des individus : ne pas porter atteinte à l'identité humaine, aux droits de l'homme, à la vie privée,

[292] Une affaire qui a fait couler beaucoup d'encre et qui, en effet, présentait un aspect croustillant. Mais les observateurs ont souvent taxé de puritanisme à cause de l'aspect sexuel. Or, en réalité, ce n'est pas tellement cet aspect qui valait une opprobre moral au Président américain que le mensonge.

aux libertés individuelles ou publiques[293]. Une attention particulière y est accordée quant aux données relevant de la santé, ou des origines raciales, tout comme des opinions religieuses ou politiques. Il est interdit de les conserver en mémoire.

294. Le principe de la législation française est fixé, en 1970, à l'article 9 du Code civil qui rappelle le droit strict de chacun au respect de sa vie privée. On donne souvent en exemple l'affaire Hallyday / Lacambre. Valentin Lacambre est à l'origine de la création, dès 1991, du service minitel « 3615 INTERNET » qui permettait de se connecter à l'Internet via un minitel. Ce qui est aujourd'hui dépassé, mais à l'époque fut novateur et lucratif. De sorte qu'il put, l'année suivante, lancer le service d'hébergement de sites web *Altern.org1,2,3*.

295. Quelques années plus tard, en 1998, Valentin Lacambre fut traduit en justice. En effet, un internaute anonyme avait publié sur son site des photos d'Estelle Lefébure ; alors l'épouse du chanteur David Hallyday, dans le plus simple appareil. Estelle Lefébure était un mannequin professionnel. Elle avait été prise en photo en privé par son petit ami du moment, qu'elle avait quitté plus tard pour épouser David Hallyday. Or, l'ancien petit ami avait fourni, au magazine Voici, les anciennes photos, sans l'autorisation d'Estelle Lefèbure.

296. Par la suite, ces photos avaient été diffusées sur le site *altern.org,* par un inconnu, qui les vait numérisé à partir d'un numéro de Voici et mis en ligne sur le site d'hébergement anonyme et gratuit *altern.org*, géré par Valentin Lacambre ; qui s'en trouvait donc être le responsable légal.

297. Estelle Hallyday poursuivit ensuite en justice l'hébergeur pour le préjudice subi du fait de la diffusion massive de ces photos sur l'Internet. Vincent Lacambre fut condamné en Cour d'appel à payer 300 000 francs de provisions sur dommages et intérêts, ainsi que 30 000 francs de frais d'avocat à Estelle Hallyday .

    Suite à cette affaire, en juillet 2000, une loi fut votée. Elle incluait un article établissant la responsabilité des hébergeurs dans ce genre d'affaires. Cependant, cet article controversé fut finalement biffé par le Conseil constitutionnel .

En 2000, puis 2002, l'Union européenne élabora des directives limitant la responsabilité des prestataires techniques, qui furent transposées dans le droit français en 2004 On peut estimer que Valentin Lacambre a été imprudent. Il a manqué de vigilance, à savoir qu'il aurait dû contrôler ce qui était sur le site dont il était l'hébergeur. Il y a eu - au moins - une responsabilité par négligence.

[293] *Loi n°78-17 du 6 janvier 1978, Loi relative à l'informatique, aux fichiers et aux libertés Légifrance.*

298. En France, l'article 777-3 du Code de procédure pénale sanctionne la tenue de fichiers nominatifs pouvant faire mention « des jugements ou arrêts de condamnation, hors les cas et dans les conditions prévues par la loi. » Evidemment, dans certains cas, cette sévérité officielle du législateur sur le sujet relève du vœu pieux .

On peut en effet s'interroger sur le caractère réellement dissuasif de mesures trop clémentes : par exemple, d'amendes insuffisamment élevées (en particulier au regard du gain éventuel), notamment de photos prises par des paparazzi. On peut même considérer que la pratique devient alors totalement hypocrite ; dès lors que la partie lésée (bénéficiant de dommages et intérêts) reçoit un montant d'indemnisation inférieur- souvent nettement - à ce que la partie coupable a réellement gagné par la diffusion de photos illégalement prises et publiées.

299. Toujours est-il que la législation européenne suit, du reste, l'orientation prise par la France, avec un peu de retard. Ce qui est facilement compréhensible, lorsqu'il s'agit d'un échelon supérieur. Le 28 janvier 1981, une Convention est adoptée à Strasbourg par le conseil de l'Europe. Elle précise, dès ses premières dispositions, que : « Le but de la présente convention est de garantir sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant. »

300. La portée de cette Convention se veut très large. Même une revue confidentielle peut être justement lue par ceux qui s'intéressent à une personne et cherchent à en savoir davantage. Ces précisions nous aident à mesurer combien le discernement du risque d'indiscrétion est chose délicate, très difficile à quantifier.

Une seule personne mal intentionnée (ou inconséquente) peut ensuite diffuser ou déformer une information. Avec des conséquences considérables à l'arrivée. Ces cas très concrets et récurrents nous donnent au moins à comprendre qu'en matière juridique, une disposition commune doit être relayée dans chacun des pays par leur propre législation nationale. Il est vrai qu'en Europe cette orientation restrictive est largement dominante et se retrouve dans les pays suivants : l'Allemagne, l'Autriche, le Danemark, l'Espagne, la France, l'Irlande, l'Islande, le Luxembourg, la Norvège, le Royaume-Uni et, enfin, la Suède .

301. Dans le cadre de l'Union européenne, le 24 octobre 1995, le Parlement européen comme le Conseil adoptent une directive « 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 ». Cette directive caresse un but bien précis : « une protection équivalente de haut niveau dans tous les Etats membres de la Communauté afin d'éliminer les obstacles aux échanges des données nécessaires au fonctionnement du marché intérieur. »

302. Deux ans plus tard, une autre directive en date du 15 décembre 1997 s'ajoute « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. ».

    L'enjeu de la protection des données à caractère personnel est devenu tel que cette exigence est - plus ou moins - considérée comme un principe constitutionnel par la plupart des pays européens. Ceci, même si la transposition concrète de ce principe dans des mesures juridiques plus particulières n'est évidemment pas identique en raison du contexte de chaque pays : si l'on ose le dire, de son " logiciel juridique " bien spécifique.

303. La directive européenne entend bien remédier à une certaine disparité : en cherchant à harmoniser la collecte, la détention, la conservation, la mémorisation des données. Ce qui n'est pas chose aisée. Lors même que le principe inspirateur s'avère identique, du moins en théorie.

    Quant aux utilisateurs des données, il leur est bien entendu clairement reconnu le droit de connaître l'origine des données en question, mais aussi, dans la mesure du possible, l'identité de l'organisme qui les traite, ainsi que les finalités de ce traitement. Il ne fait aucun doute – c'est au demeurant la moindre des choses – que les individus doivent de toute façon se voir reconnaître le droit d'accès aux données à caractère personnel les concernant. Ce droit est obligatoirement complété d'un autre : celui de demander et d'obtenir la rectification des données personnelles inexactes ou fausses. Surtout si elles entament gravement sa réputation.

304. Sont ainsi définis deux droits fondamentaux sur lesquels s'appuient des décisions supplémentaires, en particulier pour empêcher toute utilisation de ces données. Il est important de souligner un devoir de vigilance : la protection des données ne doit pas seulement concerner celles dont la divulgation serait actuellement dangereuse, mais également celles qui semblent pour l'heure anodine (ou inoffensive) mais qui peuvent un jour cesser de l'être, par exemple dans le contexte d'une dictature.

    Même s'il n'y a pas d'intention de lui nuire, le simple risque d'une potentielle utilisation néfaste est suffisante à justifier un interdit juridique. Le consentement explicite de la personne

concernée semble à cet égard vraiment incontournable et constituer l'axe central de toute législation en la matière[294]. Autrefois, dans le contexte d'un cadre de proximité, des rumeurs, du reste vraies ou fausses, pouvaient aisément se répandre. Désormais leur diffusion est beaucoup plus vaste, efficace et surtout rapide (à la limite presque instantanée, sur les réseaux sociaux).

305. La problématique se complique un peu lorsqu'il s'agit de données à caractère personnel, utilisées dans le but d'informer le public. Ce qui semble constituer aussi une certaine exigence déontologique, en particulier pour les journalistes.

En matière de création artistique ou d'œuvres littéraires, la question se complique encore davantage. On peut estimer que la directive européenne cherche une sorte de point d'équilibre entre le droit à la liberté d'expression et celui de la protection de sa propre vie privée[295]. Le droit semble affronter ce que la philosophie morale reconnait de plus en plus, à savoir un dilemme moral[296]. Ce dernier n'est pas simplement un choix difficile. L'existence d'un tel choix relève bel et bien d'une sorte d'évidence incontestable.

306. Dans le cas d'un choix difficile, il est en principe possible, bien que justement difficile, de discerner une priorité ; une solution qui s'impose. Les difficultés sont solubles. Dans le cas d'un véritable dilemme, il en va tout autrement.

Il n'y a pas moyen de parvenir à un choix véritablement satisfaisant et harmonieux. En effet, les deux exigences en conflit ne peuvent se réconcilier. Il n'est légitime de sacrifier ou de subordonner aucune d'entre elles. L'un des exemples souvent cités, à tort ou à raison d'ailleurs, est celui de l'aide au suicide éventuellement concédée à un malade incurable. En effet, aucune des deux réponses données ne sont satisfaisantes. Les deux portent atteinte également à un sentiment et un devoir.

---

[294] Anne-Laurent STERIN, « Le point sur les données à caractère personnel » *https://ethiquedroit.hypotheses.org/1717; Nicolas TILI*, « La protection des données à caractère personnel » *Nicolas Tilli in Documentaliste-Sciences de l'Information* 2013/3, 62-69 ; Nicolas OCHOA, *Le droit des données personnelles, une police administrative spéciale, thèse, 2014, Paris 1, disponible en suivant le lien https://tel.archives-ouvertes.fr/tel-01340600 [archive]* ; Ludovic COUDRAY*, La protection des données personnelles dans l'Union européenne: Naissance et consécration d'un droit fondamental*, Paris, Éditions Universitaires Européennes, 2010.

[295] Guillaume DESGENS-PASANAU*, La Protection des données à caractère personnel*, Paris, Litec LexisNexis, collection Carré Droit, 2012

[296] Bernard WILLIAMS, *La fortune morale : moralité et autres essais*, tr. Fr., Paris, PUF, 1994 ; Ruth MARCUS, « Moral Dilemmas and Consistency », in *The Journal of Philosophy* 77, 121-136.

307. Bien entendu, le dilemme moral se vérifie aussi bien à l'échelle de l'individu (de ses choix privés) qu'à celle d'une société. C'est pourquoi le juriste est également concerné, même si, en ce qui le concerne, nous pouvons préférer parler de " conflits de devoir". Ce qui rend complexe toute formulation législative.

308. Le droit énonçant des obligations, il se heurte forcément aux conflits d'obligation. C'est précisément le caractère épineux - et parfois subtil - de ce conflit de devoirs qui complique, non seulement le travail des juristes (en quête d'un perpétuel équilibre), mais encore l'action concrète des détenteurs d'un pouvoir exécutif, en aval. Ceux-ci, ne sont jamais de simples exécutants, mais aussi décideurs dans une mesure plus ou moins large.

309. Sans aller jusqu'à poser un réel conflit de devoir, le juriste se heurte souvent à l'opacité et à l'imprécision des choses. Ainsi, en matière d'œuvre littéraire ou de film, il y a souvent toute une marge - floue du reste - entre la discrétion et la désignation explicite. De sorte qu'une personne puisse reconnaître ou être reconnue, mais sans que son nom figure explicitement, par exemple par des détails, ou une initiale (qui limite considérablement le champ de recherche et d'incertitude même si cela ne correspond pas forcément à une seule personne.

310. Il en va de même si référence est faite à l'âge d'une personne. Si celle-ci permet de la retrouver, parfois avec certitude. Si par exemple je dévoile la vie privée d'un ministre en précisant qu'il est né en telle ou telle année, l'allusion est souvent transparente !

    Pourtant, le nom-même n'est pas mentionné : simplement il est facile à un esprit délié de retrouver de qui il s'agit, par exemple en consultant les fiches Wikipédia sur l'Internet. On ne peut négliger l'effet du recoupement d'informations : si je dévoile la corruption d'un ministre de cinquante ans environ, et que je dis également, qu'il vit dans telle région, je rends plus transparente l'information. Cela n'est évidemment pas vrai (ou du moins s'avère moins vrai) lorsque je parle de quelqu'un à peine connu ; ou dont les données correspondent non pas à une personne, mais à un nombre suffisamment important de gens. De sorte que l'identification devient improbable. Par exemple, si je parle d'une femme d'origine modeste, de 52 ans et vivant à Paris. Faute d'autres éléments de reconnaissance, il est pratiquement impossible de savoir s'il s'agit de telle personne que l'on connaît, ou d'une autre.

311. Du reste, quelquefois, même lorsqu'un nom est révélé, il reste loisible de dire qu'il s'agit en fait d'un homonyme, surtout lorsque le patronyme est très répandu comme Martin en France, ou Rodriguez en Espagne. Seuls d'autres indices pourraient conduire à une vraie identification.

Or, le pourcentage de possibilité ou de probabilité d'une identification est chose difficile à évaluer.

312. Il tient aussi à la diffusion du support impliqué : une allusion dans une revue papier au tirage confidentiel risque moins de conduire à l'indiscrétion, qu'un texte publié sur internet. Toutefois, là encore, le discernement juridique se révèle plus complexe entre " le dangereux " et " l'acceptable ", " le toléré " et " l'interdit ".

Elles sont aussi mouvantes. En effet, une publication confidentielle peut tout à coup cesser de l'être ; par exemple, en cas de notoriété subite d'un auteur. Il n'est jamais possible de connaître (ou de prendre en compte) tous les paramètres avec une certitude absolue. Nous sommes toujours condamnés à une certaine indétermination et à une relative incertitude ; avec - à la clé - de graves conséquences toujours, si l'on a minimisé un risque (même faible au départ). A moins de vouloir systématiquement interdire toute allusion, ce qui est impossible et inhumain, il y a toujours le risque d'une référence transparente même minime.

313. L'essentiel, pour le juriste, est qu'il soit le plus limité possible. Le problème se corse singulièrement dans la mesure où l'Internet est à l'échelle du monde entier ! Il faudrait assurer une protection identique dans tous les pays de la planète. Ce qui relève aujourd'hui d'une véritable gageure, voire d'un vœu pieux.

Une fois encore, est mise en évidence la nécessité de traiter les questions au niveau international. Toutefois, ce qui paraît relever de l'idéal se présente également comme une sorte de condition de protection réelle et efficace des données. Si celles-ci sont exportées ou piratées, et que le pays où elles se trouvent également venaient à ne pas pratiquer la même politique (le même droit) les concernant, le risque est important qu'on puisse - de partout ou presque - y accéder de façon détournée (au prix de quelques efforts).

314. Cela est encore plus immédiat pour des entreprises multinationales ayant des établissements dans les pays protecteurs et dans les pays non-protecteurs. Ils peuvent très facilement se partager les informations d'un établissement à l'autre.

Il semble bien que la directive de 1995 ait pressenti le problème. Une nouvelle notion se met en place (en définitive assez floue à cerner et à impossible à quantifier) dont on comprend la signification et l'enjeu, celle de "l'équivalence de la protection".

On peut citer dans cet esprit l'article 25.1 de la directive de 1995 décide : « Les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que

si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat. » Comme il faut forcément aller plus loin et ne pas en rester à des considérations trop générales, l'alinéa 2 du même article croit bon d'ajouter : « Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées. »

315. Pour éviter l'interdiction, il faut donc opter pour un certain protectionnisme en matière de communication ou d'échanges de données. Cela revient à interdire le transfert des données personnelles vers des pays tiers qui n'offriraient pas une protection adéquate. Le contrôle doit être assuré par les services de la Commission ; et aussi, dans une moindre mesure, par les différents Etats membres. Dès lors, on peut prendre conscience des difficultés d'un tel contrôle, outre l'investissement en énergie, en temps et argent. Un échec semble difficile à éviter. L'appréciation des risques encourus, en cas d'exportation de données personnelles vers des pays tiers, au regard de leur niveau de niveau de protection, n'est pas toujours évidente à déterminer.

    Ceci, d'autant plus que la sincérité et la fiabilité effective du contrôle ne sont pas toujours au rendez-vous. Il est en partie aléatoire, conditionnée aussi par des intérêts pragmatiques, dont il faut encore une fois peser l'importance.

    Or, le corpus législatif de référence n'est pas " très prolixe " dans la directive. Il se limite, et pour cause sans doute, à donner des critères trop précis, mesurables. Tout doit donc se décider au cas par cas. Ce qui limite donc l'efficacité, mais aussi ralentit toute action. Par exemple, l'alinéa 2 de l'article 2 de la même directive donne le droit à la Commission européenne de constituer des listes blanches ou noires, en fonction de la législation interne du pays, ou du caractère sensible, et parfois dangereux, de l'information échangée.

    Il n'existe pas une sorte de " table de multiplication" permettant de s'orienter en la matière et de déterminer des normes partout applicables. C'est au travers - sans doute, de rapprochements opérés ou d'oppositions constatées, qu'une décision peut être prise, relevant toujours d'une sorte de probabilité, grevée qui plus est d'un taux d'incertitude énorme en regard de possibilités techniques inattendues qui peuvent surgir demain, et très vite

316. Chaque secteur est traité séparément. Le secteur financier est privilégié. Certainement en raison des conséquences et des implications. D'autres semblent moins protégés, comme celui des goûts ou opinions des individus. Un peu au prétexte que cela finit de toute façon par se savoir, et se laisse deviner. Ou encore, parce qu'en démocratie, on vit – en principe – dans le respect des vues divergentes des uns et des autres. Parfois dans une sorte d'indifférence, surtout dans les espaces très urbanisés, existe par rapport aux mœurs ou aux pensées d'autrui, sauf cas limites et extrêmes bien entendu (pédophilie, racisme, terrorisme…).

Toutefois, ce relâchement de l'attention n'est pas bon. Il faut - au contraire - redoubler de vigilance. En effet, rien ne nous garantit absolument qu'un climat de tolérance perdurera indéfiniment. Le droit doit aussi protéger les individus en fonction de risques futurs, à anticiper en quelque sorte, et aussi de dérives marginales.

317. Un fanatique isolé suffit à rendre périlleuse la divulgation d'une information, par exemple. Comme souvent en droit, la directive de 1995 prévoit néanmoins un certain nombre de dérogations à ces mesures de protection. Ce qui peut donner le sentiment d'une certaine casuistique, qui n'est pas de très bonne foi. Ces dérogations sont énoncées à l'article 26 de la directive. Il s'agit du consentement de l'intéressé ; l'exécution d'un contrat entre l'intéressé et le responsable du traitement ; la nécessité de transfert de données pour l'exécution d'un contrat conclu dans son intérêt entre le responsable du traitement et un tiers ; le transfert nécessaire ou obligatoire afin de sauvegarder un « intérêt public important » ou pour « la constatation, l'exercice ou la défense d'un droit en justice » ; la sauvegarde de « l'intérêt vital » de la personne concernée ; et enfin le transfert à partir d'un registre public si les conditions légales de sa consultation sont remplies.

318. L'idée centrale, comme nous l'avons déjà souligné plus haut, demeure celle du consentement, certes éclairé, mais également responsable. En d'autres termes, cela veut dire que personne ne peut se plaindre d'une conséquence d'un choix de sa part ; pourvu qu'il ait été éclairé et conscient.

À cet égard, l'article 27 de la directive préconise l'élaboration de codes de conduite : « Les Etats membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les Etats membres. » Une mise en garde importante est ajoutée : tout cela doit être soumis à un contrôle très rigoureux. Pourtant, on peut se demander si ces codes sont suffisamment spécifiques, quant à la nature exacte ou à leur force contraignante. Ce qui en limiterait la portée effective.

319. Une critique est, ainsi, formulée en ces termes par un juriste, Guy Braibant : « rien n'est dit sur la valeur juridique et la force contraignante des codes, qu'ils soient nationaux ou communautaires, ni sur les effets de leur examen par les autorités de contrôle. Ce silence peut être interprété comme autorisant une distinction entre deux catégories de codes de conduite : les codes purement privés, élaborés et appliqués par une profession, et les codes homologués»[297]. Toujours est-il qu'un tel flou juridique pourrait être interprété comme le révélateur d'une difficulté à établir quelque chose de clair, de précis, de général.

320. Il convient toutefois de faire un constat :celui de la mobilisation de la conscience européenne sur le sujet. Sans aucun doute, le " Vieux continent " considère comme prioritaire la protection de la vie privée ; bien davantage que celle de la liberté d'expression. Il y a là certainement, du reste, une différence de sensibilité transversale à différentes questions, entre un primat juridique - et d'abord - axiologique de la liberté, du côté américain ; et un accent plus fortement porté à la protection des personnes, du côté européen.

    Ainsi, le travail du juriste consiste également à tenir compte des différences de sensibilités, séculaires parfois, tout en ayant l'ambition d'en redimensionner certains aspects. L'autorégulation à initiative privée est beaucoup plus valorisée aux Etats Unis qu'en France. La différence ne tient pas seulement à l'Océan qui sépare les deux mondes, mais certainement aussi à un clivage entre le monde latin et le monde anglo-saxon. Il ne faudrait cependant pas croire l'Amérique comme étant totalement indifférente à une certaine protection des données et de leur confidentialité. Même si cet aspect ne semble pas premier chez elle.

321. Il existe un document de la Présidence américaine, à l'époque de Bill Clinton, en 1997, intitulé « *A framework for global electronic commerce* », dans lequel il est très énergiquement rappelé que la liberté de circulation de l'information doit être protégée, et qu'un équilibre doit être trouvé entre cette liberté et la protection des droits individuels.

    Du reste, pour que toute équivoque soit définitivement écartée, le document américain n'hésite pas à critiquer non seulement les politiques du continent, mais jusqu'à la directive européenne présentée comme susceptible de conduire à des stratégies politiques disparates et éclatée[298].

322. Le même document américain parle bien d'une spécificité américaine du traitement de la question de la protection de la vie privée, dans un grand souci de flexibilité. Il n'est pas besoin

---

[297]] Guy BRAIBANT*, Données personnelles et société de l'information, rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46*, Paris, 1998, p. 124 : *https://www.idref.fr/026749610*

[298] Ira C. MAGAZINER, Ann GRIER CUTTER, Len A. COSTA, « Technology and International Policy : Essays on the Information », in *Journal of International Affairs*, 51/2, 1998, 527-538.

de préciser que Washington trouve la réglementation française et la réglementation européenne bien trop contraignantes.

L'une des difficultés les plus délicates tient bien entendu au fait que le droit européen ne s'applique pas aux consommateurs européens dans la mesure où l'entreprise n'est pas domiciliée en Europe, ce qui complique particulièrement les choses et permet bien des échappatoires. Une nouvelle règlementation pourrait être envisagée. Elle viserait à éviter un tel contournement des principes européens, à faire en sorte que la législation européenne s'applique également lorsque l'entreprise n'est pas établie en Europe ; dès lors qu'elle commercialise des produits auprès des consommateurs européens. Cependant, là encore, la solution semble incertaine. En effet, tous les consommateurs d'une même entreprise ne sont pas tous du même continent " Comment faire accepter facilement une différence de traitement juridique aux uns et aux autres ? " Ainsi, un certain flottement quant à l'avenir, et à l'option qui s'imposera en matière de protection des données (soit de moindre restriction, soit au contraire de restriction beaucoup plus dur) n'est pas dissipé. Il ne manque pas, bien entendu, de placer dans un état d'hésitation ceux qui veulent lancer des entreprises liées aux *Big Data*. Ce qui présente des risques importants en matière juridique. Dans la mesure où les bonnes pratiques ne sont pas entièrement délimitées par rapport aux pratiques illégales.

323. Trop d'incertitude quant à ce qui est autorisé (et à ce qui sera défendu) crée une tension anxiogène, dissuasive pour entreprendre. Elle favorise en revanche les entreprises illégales et la criminalité, comme nous le soulignerons plus tard. En outre, les stratégies de contournement de lois potentielles s'affinent aussi et se multiplient.

L'esprit éventuellement " tatillon " des futures dispositions européennes laissera-t-il un avenir aux entreprises européennes en la matière ? Sans doute le droit européen peut-il être un formidable levier de croissance, mais quelquefois aussi un frein à des évolutions aussi inattendues que positives.

324. On peut le juger trop strict, trop formel, et quelquefois inadapté en comparaison avec les codes de bonne conduite à l'américaine. Le problème le plus profond tient cependant, me semble-t-il, au fait que nous gardions à l'esprit une conception vraiment obsolète de données à conserver uniquement dans un but précis, et partant pour une durée précise, elle aussi limitée, alors que nous évoluons dans un monde en devenir et qui se fixe des buts eux aussi évolutifs. Nous restons fidèles à ce que l'on pourrait appeler le principe de finalité, à savoir un lien entre la collecte, la détention et la conservation des données et un usage bien particulier que nous entendons en faire, et qui légitime, de façon temporaire, de semblables opérations.

Or, aujourd'hui, des initiatives semblent être menées dans des buts éventuels, parfois contradictoires ou difficiles à accorder. Le monde numérique qui nous entoure se présente comme un espace diffus de circulation et de prolifération, assez difficilement contrôlable, surtout en regard d'échanges de données non finalisées de façon stricte et non pas, d'emblée, limités et encadrés.

Pourtant, le principe de finalité semble ici de première importance. Il doit veiller à ce que les données personnelles soient bel et bien collectées pour des buts bien précis (bien déterminés, explicites) et légitimes. Cela signifie également que les données collectées ne puissent absolument pas être utilisées à d'autres fins. Certainement pas à des fins qui seraient en contradiction avec ces buts définis au départ. On peut dire que toute décision juridique en la matière devrait de toute façon, et ce de manière systématique, bien spécifier les buts dans lesquels les données sont collectées. Par ailleurs, elle devrait mentionner les risques (plus ou moins inévitables) de détournement possible de leur utilisation à d'autres fins.

325. En ce sens, une juste compréhension et une meilleure application du principe de finalité supposent non seulement une clarté parfaite (au sujet des finalités recherchées), mais un combat contre toute déviation possible. Des garanties contre le risque d'une utilisation à d'autres fins doivent être clairement précisées, tant dans leur nature que leur contenu. En effet, le consentement éclairé d'une personne - dont les données sont collectées - suppose et implique une information sur la ou les finalité(s) choisie(s), mais aussi sur les risques de détournement de finalité.

326. Quant à la finalité retenue pour la collecte, elle ne doit pas être vague, mais bien circonscrite et aussi être justifiée de façon documentée. Toute information doit pouvoir être intelligible, et ainsi comprise de celui dont on prélève les données.

Les choses sont cependant un petit peu plus complexes. En effet, dans un certain nombre de cas, un traitement ultérieur non prévu comme tel de façon exacte mais compatible avec les finalités présentées peut se justifier Le principe de finalité induit donc une autre notion qu'il n'est pas très facile de spécifier. Celle de la compatibilité du traitement ultérieur avec les finalités initiales. Une évaluation formelle est à envisager. Elle consiste à vérifier que les finalités initiales sont incluses dans le traitement ultérieur.

Ainsi, le traitement ultérieur constitue une sorte de développement ou de déploiement des finalités initiales. Lorsqu'une telle comptabilité n'est pas évidente, il faudra soit renoncer à

l'utilisation soit adopter des mesures complémentaires telles - entre autres - que l'apport d'informations supplémentaires à la personne concernée. Dans certains cas, l'incompatibilité est évidente. Cela advient souvent lorsque la finalité d'une information recherchée est très limitée et très circonscrite. Par exemple, quand il s'agit de savoir qui utilise telle ou telle marque d'ordinateur pour récompenser celui qui utilise l'une d'entre elles. A l'évidence, dans un tel cas, toute autre utilisation des données est exclue. Effectivement, la limitation initiale est extrêmement précise. Elle n'inclut pas la possibilité d'un traitement ultérieur compatible. La question délicate qui se pose est celle des critères à déterminer en vue de reconnaître une telle compatibilité.

327. Nous sommes dans un domaine psychologique, philosophique et éthique dans lequel le discernement n'est pas évident. On pourrait dire qu'il s'agit de voir si les finalités explicites de collecte des données et les finalités du traitement ultérieur sont en quelque sorte associables. Mieux encore, les finalités du traitement ultérieur devraient être en quelque sorte déjà incluses de façon implicite dans les premières. Dans certains cas, en effet, on peut penser que la personne qui donne son consentement aux finalités initiales donne aussi implicitement son consentement à un traitement ultérieur (qui s'inscrit pour elle dans le prolongement).

    Ainsi, on pourrait envisager une sorte d'homogénéité entre les finalités premières et le traitement ultérieur. Néanmoins, il semble bien que cette homogénéité doive bien être acceptée comme telle : non seulement par un expert ou une autorité juridique, mais par la personne elle-même.

328. Nous sommes donc renvoyés à la singularité des choix et des contextes. Par conséquent, tout discernement doit s'attacher au contexte spécifique de la collecte et aux attentes raisonnables de la personne. On peut aussi accepter l'idée que le principe de finalité puisse connaître des exceptions comme la sécurité nationale, la défense, la sécurité sanitaire, la prévention ou la détection de graves infractions, ou d'autres raisons graves.

329. De façon plus limitée, ce principe de finalité pourrait être élargi dans certains cas à évaluer de fins statistiques, de recherche scientifique ou de recherche historique. Cependant, d'aucune façon, des fins statistiques, scientifiques ou historiques ne sauraient constituer des exceptions générales largement justifiées. Le discernement doit toujours être très prudent.

    Le principe de finalité hante toujours le droit européen de façon très forte. En droit, le principe de finalité déterminée revêt une grande importance. Ce principe de base stipule que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et

légitimes, et ne sauraient en règle générale être exploitées dans une perspective qui n'était pas celle voulue au départ et qui a présidé à leur collecte[299]. Et encore moins utilisées dans un but incompatible avec cette ou ces finalités. Le fait que le traitement de données à caractère personnel soit mis en œuvre pour d'autres finalités que celles pour lesquelles les données ont été collectées initialement ne constitue pas en soi une sorte d'empêchement absolu. Si et seulement si ce traitement est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement.

330. Au fond, le principe de finalité est lié au principe de compatibilité et de cohérence entre un projet initial et des éléments qui s'ajoutent et qui le modifient. Ce principe n'est du reste pas toujours facile à discerner et à mettre en application dans des matières délicates et des cas complexes. Quelquefois, pour y déroger, on peut demander aux personnes concernées un consentement préalable autorisant l'utilisation des données également dans le cas de nouvelles finalités dont il n'est pas nécessaire de vérifier la compatibilité avec les finalités de départ, même si les garanties d'une certaine cohérence s'imposent toujours. Elles pourraient, par exemple, être données par l'exigence de respect des normes de l'union européenne. Les normes techniques concernées supposent un esprit différent et surtout induisent un esprit différent, dans un espace ouvert et eclaté, polymorphe et imprévisible. Celui-ci n'est pas orienté vers un seul but clairement défini, mais articulé autour des intérêts multiples et d'ordres multiples.

331. Longtemps en France (vieil Etat de Droit de de tradition jacobine) l'État se présenta comme l'acteur majeur et le gardien unique de l'informatisation de la société. Un acteur au rôle d'autant plus décisif et crucial qu'il doit - en quelque sorte - se fixer à lui-même des limites pour garantir la vie privée des personnes. En effet, il est la seule puissance capable de s'autoriser des intrusions, mais non en dehors du cadre de la loi. La confiance en l'Etat est souvent ébréchée et " ringardise ". Les différents acteurs indépendants se multiplient. Moins coercitifs que l'Etat, mais peut-être plus dangereux, si l'on ne parvient pas à les contrôler.

332. Le développement de la cybercriminalité d'une part et d'autres crises comme celle du Covid-19, peuvent inciter à des replis sur soi, ainsi qu'à la nostalgie de frontières étatiques jugées protectrices, à tort ou à raison. La réflexion juridique ne se présente donc plus comme visant à déterminer de façon claire quelle sorte de conservation des données est légitime, comme s'il s'agissait d'une opération presque exceptionnelle, ou, du moins, ni quotidienne, ni ordinaire,

[299] Aurélien BAMDé et Julien BOURDOISEAU*, Le droit dans tous ses Etats. Le principe de finalité* : https://aurelienbamde.com/2018/12/14/rgpd-le-principe-de-finalite/ ; Nathalie MALLET-POUJOL*, Protection de la vie privée et des données personnelles* : *: http://www.clg-pergaud-maurepas.acversailles.fr/IMG/pdf/ViePrivee.pdf*

mais plutôt comme une recherche d'équilibre, dans un contexte de données abondantes, entre des exigences en tension. En effet, il est évident que des garanties très fortes de protection de la vie privée conduisent en effet à limiter la durée de conservation des données, ce qui réduit de toute façon la matière première disponible, et conduit à un appauvrissement objectif. Or, dans le cadre de certaines recherches, médicales ou technologiques, il est hautement souhaitable et fructueux de disposer d'un nombre maximal possible de données.

333. Le monde numérique d'aujourd'hui diverge aussi de celui d'hier. Il est davantage vertical qu'horizontal. La rareté des données, la difficulté concrète pour identifier nombre d'entre elles et ensuite les sauvegarder, contribuaient à l'édification d'un monde structuré, moins complexe, hiérarchique et pyramidal.

334. Les données étaient en particulier surtout conçues pour être enregistrées et vérifiées par l'autorité légitime ; non pas considérées comme une mine d'or dans laquelle beaucoup d'acteurs différents pourraient puiser (plus ou moins à leur guise). La possession des données était liée à une sorte d'autorité, presque sacrée.

335. De nos jours, un même instrument peut donner de multiples indicatifs à l'instar du téléphone portable que nous avons dans notre poche. Il sert de moins en moins, surtout dans les jeunes générations, à passer des appels téléphoniques et à y répondre. On pourrait donner un autre exemple qui vient sans doute moins spontanément à l'esprit : celui du compteur électrique intelligent. Il ne mesure pas seulement la consommation électrique, mais peut piloter à distance la climatisation ou éteindre et allumer certains appareils. La plurifonctionnalité permise par la révolution numérique, qui ne cesse de se multiplier, se heurte en définitive à un schéma rigide de segmentation des fonctions qui préside souvent à l'organisation. On peut noter - au demeurant - que ce constat s'applique aussi à la vie professionnelle. Une pluralité de tâches, un éclatement de l'emploi traditionnel et une multiplication des modifications d'un cahier de charges y imposent également une refonte des modèles rigides qui continuent à s'imposer[300].

336. La société et l'entreprise ne peuvent plus fonctionner en silos ; alors que l'organisation administrative continue à perpétuer ce modèle[301]. L'expression de fonctionnement en silo est de plus en plus souvent utilisée au Québec, et désormais en Europe, pour désigner un défaut de fonctionnement harmonieux et articulé. Ceci, dans la mesure où chacun des éléments d'une

[300] Nicolas COLIN et Henri VERDIER, *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*, Paris, Armand Colin, 2015.
[301] *Fonctionnement des entreprises par silos : un concept old school* ? http*://www.marketing-professionnel.fr/pratique-pro/fonctionnement-entreprises-silo-organisation-201204.html*

structure organisationnelle fonctionne de manière autonome, et parfois même cloisonnée, sans lien étroit ni partage d'information avec le reste de l'organisation. A l'évidence, un tel type de fonctionnement n'est pas très opérant voire handicapant. Il est heureusement mis en cause à l'ère du digital qui bouleverse l'organisation du travail. Ceci, au profit d'une meilleure visibilité et collaboration entre les services comme exprimées par des bureaux en *Open-space*.

337. On le sait, partant d'une répartition stricte des charges et d'une distinction tranchée des compétences (donc dérivant d'une démarche plus analytique que synthétique), le fonctionnement en silos implique que chaque service travaille de façon spécialisée sans se soucier des autres. C'est oublier que la synergie n'additionne pas seulement les atouts, mais les multiplie.

338. Dans un tel schéma, les différents services communiquent très rarement entre eux. Ce qui peut engendrer des pertes de temps et d'énergie. Il correspond bien à un système hiérarchique et à un management de type pyramidal. C'est-à-dire que les décisions sont descendantes tandis que le niveau de responsabilité est ascendant.

339. Frappé d'obsolescence, le système de fonctionnement par silos continue toutefois de survivre, en particulier dans le cadre des administrations publiques. Peut-être parce qu'il est plus rassurant pour certains. Les nouveaux moyens de consommation suscités par le digital le mettent bien entendu fortement en question. Les attentes qui se multiplient ne trouvent pas de réponses rapides ou satisfaisantes lorsque le fonctionnement est retardé ou bloqué par le fonctionnement en silos.

340. Cependant, ce dernier trouve encore des défenseurs pour les raisons qui suivent. Ce fonctionnement en silos structure mieux les tâches spécifiques de chaque employé. Il évite le stress et présente une indéniable cohérence logistique. Toutefois il incarne bien une forme d'organisation habituée à une verticalité des décisions, à une structure bien établie, à une division des compétences et des approches au détriment de la transversalité. Il semble de moins en moins adapté à la fois au numérique et aux jeunes générations. On peut raisonnablement penser que les tâches doivent être mieux coordonnées et leur répartition moins stricte.

341. L'urgence d'une réforme des normes qui régissent la société et le travail devient chaque jour plus évidente. Trop poser des conditions draconiennes au départ, mettre des freins trop serrés, corseter les activités de manière paralysante ne peut qu'empêcher un pays de se développer, tandis que d'autres le feront ailleurs. Du reste, il y a fort à parier qu'une rigidité excessive, outre

son aspect néfaste et paralysant, finisse par susciter, en compensation et par réaction bien compréhensible, l'effet inverse de celui recherché. A savoir des transgressions de plus en plus nombreuses et à chaque fois plus subtiles. Une sorte de désordre qui n'est pas un chaos initial encore à structurer, mais plutôt une sorte de dérèglement d'un ordre initial trop rigide et mal adapté, souvent plus fantasmé que réel.

342. En définitive, c'est une régulation complexe et bien entendu très sophistiquée des algorithmes qui semble devoir s'imposer[302]. Il conviendrait, ainsi, de forger un droit des algorithmes. Nous en sommes encore loin. L'ambition est réelle, mais paraît s'imposer. Ainsi, il ne s'agirait pas de détruire des données. Ce qui constitue une perte objective souvent dommageable, mais plutôt de réguler l'utilisation qui pourrait en être faite.

343. Trois principes pourraient être les piliers de ce droit. En premier lieu, le principe de tolérance, qui demande de rendre un algorithme accessible à tous. En second lieu, un programme algorithmique devrait être certifié par des experts compétents et indépendants. Enfin, en troisième lieu, il importe d'honorer un principe de contestabilité de l'algorithme. Ce qui nous préserverait d'emblée de toute sorte d'usage totalitaire. Des mesures imprécises et floues, ou au contraire trop rigides, ne peuvent que bloquer l'avancée d'un pays, au niveau économique. Or, il se trouve que d'autres pays, dans une sorte de concurrence mondiale, risquent bien de ne pas l'entendre de cette même oreille. Au contraire, ils vont tirer profit d'une politique inadaptée de celui qui se présente alors comme un rival distancé.

344. Dans le contexte de mondialisation qui nous entoure et que nous ne pouvons nier, par rigidité ou manque de précision et de professionnalisme, il ne fait guère de doute que celui que se mettra à la traîne sera un perdant, et sera distancé[303]. C'est aussi la raison pour laquelle, dans le monde globalisé qui est le nôtre, l'une des formes que prend la compétition entre entreprises (et aussi entre pays) est la concurrence juridique. Il faut certainement réguler, mais non pas en s'enfermant dans une sorte de carcan en retard sur le monde actuel.

---

[302] Adrien BASDEVANT et Jean-Pierre MIGNARD*, L'empire des données. Essai sur la société, les algorithmes et la loi*, Paris, Don Quichotte, 2018. Sur la nature même des algorithmes : Patrice HERNERT, *Les algorithmes*, Paris, Presses universitaires de France, coll. « Que sais-je ? », 2002.

[303] Ce que montre très bien : Luc FERRY et Nicolas BOUZOU, *Sagesse et folie du monde qui vient. Comment s'y préparer, comment y préparer nos enfants,* Paris, Plon, 2019.

Cette concurrence juridique suppose précisément une attention constante à la recherche d'un équilibre entre la protection des données et à la volonté de ne pas en perdre. Ce qui plomberait la recherche et l'innovation.

345. En ce qui concerne les Emirats, de façon plus spécifiques, la nécessité de légiférer en matière de protection des données a émergé un peu plus tardivement qu'en France ou qu'aux Etats-Unis. Du point de vue juridique, les Emirats ont adhéré en 1974 à l'Organisation mondiale de la propriété intellectuelle, ainsi qu'à la WIPO Lex (relative à la propriété intellectuelle et à la conservation des données). Suivant les orientations de ces deux instances, les Emirats préservent le plus possible les données personnelles. Toutefois, ils doivent encore prendre des décisions plus concrètes dans le détail.

346. C'est - du reste - pour cette raison que notre recherche est fortement orientée sur la préconisation. Les grandes orientations entrent parfois en conflit entre elles. Il est alors nécessaire de trouver des solutions équilibrées et médianes. Toutefois, les Emirats ont déjà mis en place, et continuent à mettre en place un cadre[304] dans lequel pourra s'affiner ensuite une régulation - beaucoup plus précise - des nouvelles technologies.

    Les principes sont ainsi définis comme stratégiques. Ils visent à déterminer, avec souplesse, des politiques concrètes. Il ne s'agit pas de trancher d'en haut - de façon rigide et figée - toutes les questions particulières, mais de permettre, dans la souplesse et l'adaptation constante, à une situation toujours mouvante de définir - peu à peu et de façon toujours ajustée, des réponses plus concrètes.

347. Ces principes juridiques fondamentaux sont - en définitive - assez simples. Ils sont les suivants. En premier lieu, toutes les lois nationales et internationales en vigueur doivent continuer à s'appliquer, même dans le cadre des nouvelles technologies numériques. En aucun cas, le cyberespace ne saurait constituer un espace de non-droit, où il serait possible de s'affranchir des législations existantes, ou du moins de les contourner adroitement. Par exemple, la stricte protection des données personnelles doit rester la même dans le cyberspace que partout ailleurs.

    Ce sont les menaces qui changent et les moyens pour protéger les données qui évoluent, mais non pas les axes juridiques. Ceux-ci ne peuvent en aucun cas être infléchis, sous prétexte d'une

[304] https://www.desc.gov.ae/cyber-strategy/

plus grande difficulté d'assurer un contrôle. Il ne faut pas créer du droit inutilement, au-delà des dispositions déjà existantes. Au risque de freiner l'innovation et l'avancée.

348. Le cyberspace doit pouvoir demeurer un univers de compétition et de concurrence, d'innovation audacieuse. Il ne saurait être paralysé par le principe de précaution. L'éducation aux nouvelles technologies doit inciter à l'acceptation d'un minimum de risque. En effet, le risque zéro n'existe évidemment pas. Dans la mesure où les menaces qui pèsent sur le cyberespace dans le cadre émirati sont transnationales, il est important de multiplier les partenariats régionaux et les accords à l'échec du monde entier.

349. L'organisation du cyberespace dans les Emirats, « The Public Key Infrastructure (PKI) » [305] permet aux divers utilisateurs, ainsi qu'aux ordinateurs, d'échanger entre eux en toute sécurité un grand nombre de données. La communication cryptée est la base de tout service efficace et du bon fonctionnement d'une smart city. En ce qui concerne la blockchain, quand la simple règle de l'anonymat ne se présente pas comme la meilleure solution, il est important de faire référence à une autorité pleinement compétente pour identifier les contrats et les usagers authentiques et acceptables qui rejoindront la blockchain. Il va de soi que la blockchain repose bel et bien sur des techniques éprouvées et légales de cryptage.

Si l'anonymat de l'utilisateur doit être préservé pendant la transaction, les technologies de la cryptographie conservent cependant la référence du lien à l'ordinateur de connexion (voire même l'ID de l'utilisateur si d'aventure cette information devait être demandée par des autorités légitimes).

350. En ce qui concerne l'Internet des objets, les certificats des appareils doivent être accessibles, et les droits des consommateurs soigneusement respectés. Chaque fois que des données sont communiquées, il doit en outre être possible de prévoir d'éventuels certificats limitant étroitement toute manipulation de ces données qui ne serait pas approuvé par celui qui les livre. Tous les protocoles d'accord se feront au maximum sous forme numérique pour éviter au mieux l'inflation de documents en papier ; qui sont de toute façon voués à disparaître avec le temps.

[305] *https://www.desc.gov.ae/regulations/public-key-infrastructure/*

351. Les Emirats entendent également mettre sur pieds des instances de régulation et de diminution des risques sur le cyberespace[306]. Le but de l'ISR (« Information Security Regulation ») est de permettre à toutes les échelles du pays de poursuivre leurs transactions d'information de la manière la plus sécurisée possible. Il s'agit de définir aussi différents degrés de sécurité et de confidentialité, en fonction de l'enjeu.

352. L'ISR se présente comme un cadre technologique en soi (neutre et indépendant), au sein duquel des activités contrôlées, légales et aussi sûres que possible peuvent avoir lieu. Il s'adresse non seulement aux services gouvernementaux (ou reliés à l'Etat), mais aussi à tous ceux qui sont légitimement amenés à entrer en contact avec ses services, y compris dans le contexte d'un contrat ou d'une simple visite.

353. En outre, il est important de souligner que ce cadre de contrôle concerne également toute information gouvernementale, peu importe le moyen de sa transmission. Le champ de compétence d'ISR se divise en treize domaines d'application. Chacun d'entre eux se soucie de l'une ou l'autre des principales catégories d'information. Les mesures prises par les Emirats s'appliquent aussi aux voitures autonomes ; qui vont certainement se multiplier dans les temps à venir de manière exponentielle.

c. ***La question de l'informatique ubiquitaire***

354. La connexion entre les objets permet un ajustement de l'offre et de la demande, à l'instar des publicités ciblées, qui nous parviennent en fonction de nos achats (et parfois de l'appréciation que nous formulons). Par exemple, c'est ainsi que fonctionnent les « *like* » de Facebook.

Outre l'indélicatesse de telles stratégies commerciales. On peut également redouter une volonté d'imposer des choix ; ou - du moins - de les influencer de façon très forte. Cela revient à surveiller ceux qui liront un panneau, pour le conditionner encore davantage. Se forme alors le problème de " l'informatique ubiquitaire " ; d'une interférence numérique *everywhere* (ou mieux *everyware,* selon le néologisme et mot-valise forgé par Adam Greenfield[307]). Après les ordinateurs personnels et les ordinateurs centraux, une nouvelle période de l'informatique s'ouvre, celle de l'informatique ubiquitaire.

[306] https://www.desc.gov.ae/regulations/standards-policies/
[307] Adam GREENFIELD *Everyware: la révolution de l'ubiquité*, tr. fr. éd. Fyp, 2007.

Celui-ci personnifie bien la troisième ère de l'histoire de l'informatique qui succède à celle des ordinateurs personnels et des ordinateurs centraux. En réalité, derrière le qualificatif un peu mystérieux d'ubiquitaire se dissimule quelque chose de très simple ; qui commence à devenir très familier : l'informatique est tout simplement omniprésent dans les moindres faits et gestes du quotidien.

355. Il s'agit d'une informatique que doit affronter, découvrir, domestiquer et potentialiser tout un chacun. L'utilisateur dispose désormais de toute une gamme de petits appareils informatiques, connectés entre eux, qui facilitent l'échange de données et d'informations. Ceci, quelle que soit la localisation des personnes. Au Japon, on parle quelquefois de " réseaux omniprésents ". Le smartphone, ou l'assistant personnel, nous en donne une idée, faible encore. Même si le phénomène est relativement invisible, mais non moins décisif et marquant.

356. L'un des pères de l'informatique ubiquitaire est Mark Weiser[308], un ingénieur de génie décédé prématurément à 47 ans en 1999. Ce dernier avait bien mis en évidence combien nous assistons à une révolution globale reconfigurant une sorte de nouvelle totalité articulée, en l'occurrence connectée. Weiser s'inspire beaucoup du roman de Philip K. Dick, *Ubik*.[309] Dans ce dernier, l'écrivain de science-fiction montre bien les ravages d'une absence de distance ; d'une simultanéité de tout ce qui survient. De même que certains saints, du moins selon les pieuses légendes, étaient présents non seulement en deux lieux différents (bilocation), sinon en tous (ubiquité), ainsi toute chose pourrait être un jour reliée à toutes les autres.

357. Dans l'ère de l'informatique ubiquitaire, non seulement chaque utilisateur dispose de toute une gamme d'appareils fonctionnant les uns avec les autres (comme un grille-pain qui peut se mettre en marche lorsqu'un réveil sonne, par exemple), mais les nouvelles technologies transforment cette même réalité à l'aide de nouveaux outils numériques. Ma liseuse ressemble à un livre, mais n'est plus un livre.

358. L'informatique ubiquitaire se présente comme décentralisée. Les calculs sont faits par de nombreux petits appareils. Chacun ayant une fonctionnalité qui lui est propre. Nous sortons, ainsi de l'époque des ordinateurs centraux. Lorsqu'un ordinateur central unique, très puissant,

[308] Cf. *https://web.archive.org/web/20080129083444/http://www.cs.berkeley.edu/Weiser/index.shtml*
[309] Philip DICK, *Ubik*, tr. fr. Alain Dorémieux, Paris, Robert Laffont, 1970. Pour l'importance de la science-fiction afin de progresser dans la pensée : cf. Fredric JAMESON, *Penser avec la science-fiction*, Paris, Max Millo, 2008. Cf. l'ouvrage collectif, *Spécial Philip K. Dick, Revue Science-Fiction,* 7–8 Paris, Denoel, 1986. Sous forme plus littéraire : Emmanuel CARRERE, *Je suis vivant et vous êtes morts*, Paris, Seuil, 1993 (surtout pp. 186-197).

s'acquittait de tous les calculs. Dorénavant, les diverses fonctions sont remplies par toute une gamme d'appareils.

Ainsi, l'utilisation nomade et l'utilisation internationale sont favorisées. N'importe quelle application doit pouvoir être utilisée sur n'importe quel appareil, grâce à n'importe quel réseau. L'utilisation de chaque appareil devient de plus en plus aisée, intuitive, sinon évidente. Ceci, dans le but d'une très large utilisation des produits, donc d'une commercialisation en hausse. Il est évident que leur usage va devenir de plus en plus aisé pour tout un chacun. Ce phénomène est destiné à s'accentuer. D'autant plus que les jeunes générations disposent d'une maîtrise plus aisée de ces nouveaux instruments. Certes, les nouveaux appareils des années 2010 demeurent limités en puissance et en capacité de stockage. Toutefois, des nouveaux horizons s'ouvrent dans un avenir très proche ; en particulier grâce au progrès exponentiel des technologies de communication, surtout sans fil. On peut donc prévoir, à court terme, la mise en place de logistiques collaboratives globales. Ceci, grâce au concept de nomenclatures étendues, gérant une chaîne complète de production et de distribution.

359. On peut envisager, comme le fait l'informaticien Jean-Baptiste Waldner, une transformation - dans les prochaines années - de l'ordinateur en un vaste réseau d'objets minuscules et hétérogènes formant alors une sorte d'assemblage en essaim, avec des milliards de nœuds.

Pensons simplement qu'en une journée un être humain se trouve déjà en contact avec au moins un bon millier d'objets De multiples temps et espaces d'échange se créent donc entre l'homme et les machines ; pour le pire comme peut-être pour le meilleur[310]. D'une certaine manière, la machine devient comme les humains et les humains comme des machines ; sans que l'on sache parfois véritablement lequel l'emporte et détient l'avantage sur l'autre Les philosophes et les juristes ne peuvent négliger de prendre en compte les chances et les risques d'une semblable évolution. Ainsi, selon Greeenfield, il y a un risque à induire subtilement des attitudes normatives, à créer une nouvelle forme de panurgisme. Panurge est un personnage de la littérature française, inventé par François Rabelais. Il pousse un mouton à se jeter à l'eau, de sorte que tout le reste du troupeau s'y précipite également. Les technologies de visualisation nous conditionnent déjà puissamment et induisent en nous de nouveaux codes moraux[311].

360. Cette connexion de toutes les choses et des personnes peut conduire à une société du contrôle. Elle peut faire penser au *Panoptikon* envisagé, au XVIIIe siècle, par le philosophe anglais

[310] Jean-Baptiste WALDNER, *Nano-informatique – Inventer l'ordinateur du XXIe siècle*, Paris, Hermès, 2007.
[311] Peter-Paul VERBEEK*, Moralizing Technology : Understanding and Designing the Morality of Things,* Chicago and London, University of Chicago Press, 2011.

Jeremy Bentham comme substitut aux peines de prison[312]. L'architecture remplacerait la détention carcérale. Il n'y aurait plus besoin d'enfermer les délinquants, car on pourrait sans arrêt les suivre du regard[313].

361. Se lancer avec enthousiasme dans le Big data sans poser les questions éthiques, et sans envisager des protections juridiques semble inconséquent. *L'American Civil Liberties Union (ACLU)* a exprimé sa préoccupation à propos de la capacité qu'a l'Internet des objets à éroder le contrôle que peuvent avoir les personnes sur leur propre vie. Certes, le consentement de l'utilisateur est reconnu comme une condition contractuelle, mais - concrètement - les utilisateurs n'ont pas toujours le temps, ni les moyens, ni le calme, ni la persévérance de vérifier les risques. De donner un consentement éclairé.

362. En 2007, le gouvernement britannique préconisa la mise en place d'un programme de compteurs électriques intelligents. Une mesure qui peut paraître fort anodine, au premier abord. Néanmoins, deux ans plus tard, le Parlement néerlandais a rejeté un programme similaire de compteurs intelligents, en fondant sa décision sur des préoccupations concernant le respect de la vie privée (avant de revenir sur cette décision un peu plus tard). Il semble bien qu'aucune donnée collectée ne soit anodine, même si une surconsommation peut par exemple s'expliquer de bien des manières. Il n'empêche, un utilisateur dont la consommation sera faible risque bien d'être très peu chez lui, ou presque jamais. Cette information peut être considérée comme étant privée, on en tous les cas ne regardant personne.

363. Dans un article de janvier 2014 publié dans *Forbes*, un chroniqueur en cybersécurité, Joseph Steinberg[314] a répertorié plusieurs appareils connectés à Internet qui sont hélas susceptibles d'espionner « les gens dans leur propre maison », en l'occurrence : des téléviseurs, des appareils ménagers, des caméras ou même des thermostats.

364. À ce problème de non-respect de la confidentialité s'ajoute celui d'une cybercriminalité galopante. Les hackers peuvent facilement s'en prendre à des cibles très vulnérables comme les freins ou le moteur d'un véhicule, d'autant plus que les systèmes informatiques sont connectés à internet et contrôlables à distance. Des stimulateurs cardiaques peuvent également être

[312] Jeremy BENTHAM, *Panoptique*, tr. De Christian Laval, Paris, Mille et une nuits, 2002. Cf (pour une actualization) : Pascal FROISSART, "Archivage du panoptisme. La télé-réalité sur internet" *in MédioMorphoses*, 2013, 1, 13-17.
[313] Janet SEMPLE*, Bentham's Prison, A Study of the Panopticon Penitentiary*, Oxford, Clarendon Press, 1993.
[314] Pour l'ensemble de ses publications *: ttps://josephsteinberg.com/blog-and-articles/*

contrôlés à distance ; tout comme des télécommandes de pompes à insuline et des défibrillateurs cardioverteurs implantables.

365. De même, on ne peut non plus passer sous silence les risques pour l'environnement. Dans la mesure où l'électronique utilise largement des produits chimiques et synthétiques très toxiques, et généralement fort difficiles à recycler. Ainsi, l'enjeu environnemental se révèle considérable. Tous ces dispositifs sont riches en semi-conducteurs. Ce qui exige des produits de qualité mais nocifs, parfois imprudemment incinérés (sans davantage de précautions) ou simplement stockés dans des décharges ordinaires. Le nombre de déchets semble - du reste - destiné à croître en raison de ce que l'on appelle quelquefois "l'obsolescence programmée »[315] : à savoir, la réduction voulue (et parfois drastique) de la durée de vie d'un produit, en vue de son remplacement. C'est le cas de machines à laver le linge par exemple.

366. Face à tous ces périls, une Fondation de sécurité des objets connectés a été instituée le 23 septembre 2015, dans le but de sécuriser de tels objets. Elle se compose de fournisseurs technologiques et d'entreprises de télécommunications incluant BT, Vodafone, Imagination Technologies et *Pen Test Partners*. Le marché de la sécurité est en plein essor. Il atteint jusqu'à 350 millions de dollars. Ce chiffre est voué à doubler très rapidement, en considération des avancées de plus en plus rapide. Ce qui révèle une véritable capacité d'adaptabilité permettant de trouver très rapidement des solutions adéquates.

367. L'obsolescence programmée est un délit, réprimé. C'est exactement, mais à une beaucoup plus large échelle, le même phénomène que celui de l'incitation répétée à acheter le dernier IPhone ; même si celui dont l'on dispose se trouve encore en excellent état de marche. Ce problème ne tient pas seulement à l'essor des technologies, mais également à une sorte de philosophie diffuse. Le droit, dans son élaboration, ne peut donc manquer de s'interroger sur l'idéal moral et social visé qui n'est pas forcément le même pour tous.

368. Ainsi, formant une dimension économique entièrement inédite (aux enjeux exceptionnels et aux risques inquiétants), la nouvelle configuration informatique qui se dessine, en intégrant l'Internet mondial des objets change le monde. Elle appelle à une réflexion juridique très précise dans la perspective de sauver la dignité humaine, et de faire barrage à des formes possibles de

[315] Philippe FRENAUX, « Des produits conçus pour ne pas durer », in Alternatives Economiques, 305, 1/09/2011, *https://www.alternatives-economiques.fr/produits-concus-ne-durer/00043204*

totalitarisme et de criminalité. La question revêt donc une dimension essentiellement politique ; non plus tellement technique. Ceci, d'autant plus que le développement du numérique inclut des enjeux géopolitiques évidents.

Section* II *: Un ancrage géopolitique à asseoir par le numérique.

369. La révolution numérique superpose un cyberespace virtuel avec des contours et des délimitations internes difficiles à évaluer mais également avec ses propres lois sur le monde entier.

Elle n'a pas progressé et ne progresse pas au même rythme, et de la même façon, selon les différents pays. Toutefois, il s'agit bien d'un phénomène mondial, qui semble aspirer à sa souveraineté propre, au-delà des anciennes souverainetés.

370. Par ailleurs, contrairement à l'idée d'un tout sans délimitation de départ. Cet ensemble pourrait susciter de nouveaux découpages territoriaux. Notamment, en raison des ratés d'une gouvernance mondiale induite par la nature-même de l'Internet, laquelle gouvernance renforcerait ensuite ce qu'elle était censée avoir aboli

a. Révolution numérique, gouvernance et souveraineté.

372. Comme chacun peut le constater, l'espace numérique est accessible dans pratiquement n'importe quel point du globe. Du reste, « l'idée qu'il s'agisse d'un réseau global et sans frontière, s'affranchissant des contraintes locales, territoriales, pour permettre une connexion mondiale et instantanée de ses usagers semble assez en phase avec la manière dont les acteurs initiaux de web ont conçu et pensé Internet »[316].

Ainsi, comme nous l'avons déjà précisé, l'Internet sonnerait la caducité des juridictions classiques du monde physique. Il annoncerait une indépendance acquise, et ce, de manière définitive. Les Etats se trouvent confrontés à cette universalité sans-frontière qu'est l'Internet. Ainsi, un militant des droits de l'homme spécialisé dans la traque des idéologies nazies est parvenu à imposer à Yahoo de bloquer certains contenus. Sur son alerte, la loi française oblige

[316] Armaël CATTARUZZA, « Quelle souveraineté pour l'espace numérique », in collectif, *La cyberdéfense. Politique de l'espace numérique,* Paris, Armand Colin, 2018, 83, [83-91]. Boris BEAUDE*, Internet. Changer l'espace, changer la société,* Limoges, Editions FYP, 2017 ; Alix DESFORGES, « Les représentations du cyberespace : un outil géopolitique « in *Hérodote,* 2014, 152-153, 67-81.

un serveur à bloquer les sites néo-nazis, non censurés en Amérique, sur le territoire français. Ce qui *de facto* retraçait une frontière. On pouvait parler d'une « territorialisation d'internet »[317].

373. L'idée a certainement été relancée après la grande cyberattaque subie par l'Estonie en 2007. En définitive, le monde sans frontière semble ainsi relever, malgré Internet, de l'illusion, de l'utopie ou du cauchemar, pour les uns et pour les autres. On assisterait, ainsi, à l'émergence d'un processus d'appropriation du cyberespace, ainsi qu'à une configuration de nouveaux territoires avec des incidences à plusieurs dimensions. Ils rétabliraient de nouveaux rapports de force et de nouvelles rivalités.

374. Dans cette perspective, le contrôle des données passe par l'acquisition et le développement d'infrastructures et logistiques nationales de stockage et traitement. Le caractère national est renforcé par le fait que le caractère de donnée sensible est différemment évalué selon tel pays ou tel autre.

375. Nous sommes là au croisement de choix économiques, stratégiques et politiques. Il est - de plus en plus - question d'une souveraineté numérique : c'est-à-dire, d'un contrôle national des données (mais également d'une sorte de sémantique, qui serait propre à chaque nation). En réponse à ce nouveau souci, chaque pays envisage des solutions juridiques et techniques qui peuvent être voisines, mais qui lui sont propres. C'est ce que l'on appelle la géopolitique des *datacenters*.

376. A la base de cette géopolitique se trouve une conviction - plus ou moins partagée (qui aurait pu sembler farfelue il y a un certain nombre d'années), selon laquelle on pourrait localiser physiquement des données. Cela n'implique cependant pas nécessairement une localisation nationale : elle peut être régionale, ou à l'échelle d'un continent (comme l'Europe, ou l'Union Européenne). Cependant la tendance dominante est actuellement celle de la territorialisation nationale.

    Curieusement, on peut dire qu'au souhait pour des raisons économiques d'une libre circulation des données s'ajoute une forme de néoprotectionnisme, dans l'acceptation même du recul financier qu'il induit [318]. Pour surmonter cette contradiction, l'idée serait de constituer des

[317] Jack GOLDSMITH et Tim WU, *Who Controls the Internet ? Illusions of a Bordeless World,* New York, Oxford University Press, 2006. .
[318] Neha MISHRA, « Data localization laws in a digital world » in *The Public Sphere Journal,* 2016, 135-158.

partenariats et des accords. Ce qui fait courir le risque que cela ne conforte davantage la position hégémonique des Etats-Unis.

377. En effet, la domination des géants américains du Web, sur le marché mondial, semble permettre aux Etats-Unis d'étendre l'application du droit de ce pays bien au-delà des frontières nationales. Le célèbre *Patriot Act* (adopté en 2001 suite à l'attentat des Twin Towers) autorise les autorités américaines à accéder aux serveurs hébergés sur le territoire des States.

Par ailleurs, les amendements au *Foreign Intelligence Surveillance Act* autorisent ces mêmes autorités à accéder aux données des citoyens étrangers stockées dans un cloud. Il y a même pire. Les services de renseignements américains pourraient également avoir accès aux données hébergées en Europe par des sociétés relevant du droit américain s'il y a suspicion de terrorisme. Il est vrai cependant que ces mêmes sociétés n'y sont guère favorables par crainte de perdre leurs clients. À cet égard, on peut parler d'un véritable bras-de-fer entre l'administration américaine et Microsoft de 2014 à 2016.

378. Toujours est-il que les Etats-Unis cultivent une interprétation extensive du droit dans le sens d'une possibilité élargie d'assurer la Sécurité nationale. Depuis juillet 2016, le transfert des données entre les Etats-Unis et l'Europe est encadré par le *Privacy Shield*. Celui-ci vise à mieux garantir le respect du droit des Européens à leur vie privée et à la protection de leurs données. Néanmoins, ce consensus fait davantage figure de compromis transitoire que de solution à long terme. De nombreuses exceptions sont en effet prévues à la garantie des droits des Européens. Ce qui limite la portée durable de ce compromis[319]. En bonne part en réaction à la détermination américaine, se renforcent donc des lois visant à maintenir les données sur leur propre territoire national ; sans qu'elles puissent être transférées à l'extérieur ou contrôlées de l'extérieur.

379. Dans de nombreux pays que le leadership américain n'enchante guère des législations ont été adoptées en ce sens : le Vietnam, l'Indonésie, le Brunei, l'Iran, la Chine, le Brésil, l'Inde, le Nigéria, et, bien entendu, la Russie[320]. La Russie fait tout pour diffuser un contre-message à

[319] *https://techcrunch.com/2019/12/19/more-legal-uncertainty-for-privacy-shield-ahead-of-crux-ruling-by-europes-top-court/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAHwMQXMcZs0tLGiLweUQYwgIaBQ0d_EBy8GHF019USnmlf_GoVFp_Bs0x9trebFNIMe4UXHHgu1Cw1u6ptuOd3DQqz71oknP6pofPPfzAIlDYcOb1SfNYOoIpk1XkEZwEZnZM8coVJtlhppt4uN1JO4lH_9FF0PeqzkqMf9vKJGq*

[320] Mark SUSLOV et Mihail BASIN*, Eurasia 2.0. Russian Geopolitics in the Age of New Media,* Londres-New York, Lexington Books, 2016.

l'hégémonie américaine. Elle renforce son message identitaire et la reconnaissance de ses propres valeurs. Elle oppose son soft power à l'hégémonie américaine.

La technologie du *cloud computing* [321,] qui devient une configuration prédominante, s'est développée en quelques années. Il s'agit d'un système de stockage et de traitement de l'information, rendu nécessaire par le grand nombre des données, mais également la complexification des systèmes. La gestion des ressources est confiée à un prestataire. Grâce au *cloud*, la proximité géographique n'est plus du tout un impératif. Le *cloud* n'est donc plus circonscrit par des frontières nationales. Le maillage numérique devient alors d'autant plus distinct du maillage administratif et politique. De sorte que fournisseurs, infrastructures et utilisateurs peuvent alors dépendre de souverainetés différentes! Ce qui pose évidemment des problèmes concrets.

380. La puissance américaine en sort renforcée. On assiste à une nouvelle convergence et à une nouvelle concentration des données[322]. Face à cette situation, les Etats tentent de trouver des parades ou des solutions. L'une des plus simples est évidemment de dire que les données sont soumises à la loi en vigueur sur le territoire où elles se trouvent. Ce qui donne évidemment le droit à un État d'accéder aux données qui sont hébergées par les structures situées sur son sol. La majorité des données transitent au moins un temps sur le sol américain.

381. Sur le fond, il y a quelque chose de problématique sinon d'inquiétant dans le fait qu'un gouvernement puisse aisément accéder à des données de citoyens étrangers.

L'une des pistes avancées, pour pallier cette situation, est la suivante. Un Etat devrait construire un *cloud* contenu dans des limites administratives connues ; et recourir aux services de prestataires exclusivement nationaux. Tout le dispositif devrait reposer sur des *datacenters* qui se trouvent sur le même territoire national.

382. C'est en ce sens que le gouvernement français François Fillion proposa, en 2009, la mise en place d'un *cloud* exclusivement français. Hélas, des divergences de vue en compromettent la réalisation.

Une autre piste est de trouver un pays de confiance, avec une législation semblable en la matière, et avec qui développer des certifications communes, comme l'Allemagne. Cette piste

[321] Jana ANDERSON et Lee RAINIE, « The future of cloud compujting » : *https://www.pewresearch.org/internet/2010/06/11/the-future-of-cloud-computing/*

[322] Primavera DE FILIPPI et Smari McCARTHY, « Cloud computing : centralization and data sovereignity » in *European Journal of Law and Technology*, 3, 2, 2012.

se rapproche de celle d'un *cloud* de l'Union européenne. La question du *cloud* demeure importante et en bonne partie irrésolue[323].

383. Envisager alors une gouvernance de l'Internet a-t-il seulement un sens[324], dans le cadre des crispations en cours, et du retour d'une forme de bras-de-fer géopolitique[325], en particulier entre les Etats-Unis et la Russie, et alors qu'émergent de nouveaux enjeux ?

Sans même que cette gouvernance ne soit très clairement définie, une sorte de guerre froide pour assurer une influence ou pour échapper à une hégémonie quant à cette gouvernance[326]s'installe. L'Internet exprime une transversalité. Ce qui rend cette gouvernance singulièrement indécise, improbable et pourtant incontournable. Il n'est plus possible de voir dans le numérique un seul champ supplémentaire de relations internationales structurées par des Etats. Toutefois, il n'est plus possible d'éluder davantage la dimension interétatique.

384. Lors du Sommet mondial sur la société mondial de l'information à Tunis en 2005, une pyramide institutionnelle est dressée : au sommet duquel trônent toujours les Etats mais jusqu'où contrôlent-ils encore leur base ? Il y a certainement deux polarités qui peuvent rester ou traverser les uns et les autres dans la façon de concevoir la gouvernance numérique. Certains souligneront l'aspect technique, sinon technicien, et le fait qu'une telle réalité, à l'essor et aux évolutions prodigieusement rapides, est vouée à s'autoréguler comme le marché des libéraux. D'autres, en revanche, pensent que l'Internet ne fait qu'exacerber des tensions et que renforcer des tensions à l'incontournable dimension étatique. Il serait donc nécessaire, selon eux, de revenir à des règles et à des instruments coercitifs bien connus.

385. Cependant, comment est-ce possible dans la mesure où l'Internet (en lui-même) déplace les repères, brouille les lignes et élargit forcément l'expression et la participation. La juste gouvernance serait une sorte de juste milieu entre les deux conceptions, l'une libérale et l'autre autoritaire ; mais avec le risque de ne satisfaire personne ; de bloquer au lieu de contrôler et d'encadrer positivement.

---

[323] Clotilde BOMONT, « Maîtriser le cloud computing pour assurer sa souveraineté » in *La cyberdéfense (op. cit),* 91-98.
[324] Julien NOCETTI, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » in collectif, La cyberdéfense (op. cit), 130-136.
[325] Walter Russell MEAD, « The Return of Geopolitics » in *Foreign Affairs*, 2014, 93, 3.
[326] Laura DENARDIS, *The Global War for Internet Governance*, Yale, Yale University Press, 2014.

Centre de gravité mouvant, l'Internet n'est devenu que davantage ingouvernable, chaotique, contradictoire et menaçant, condamné à une oscillation entre des tours de vis répressifs et liberticides et des dérégulations postérieures, radicales et dangereuses.

386. Reste à savoir comment peut s'organiser une telle gouvernance ; à supposer qu'on ne la laisse pas se mettre en place toute seule, même au prix de tensions et de conflits. A l'évidence cette gouvernance ne saurait être qu'internationale. Ce qui est à la fois indispensable, et semble condamner à jamais cette gouvernance à être une chimère : tant une synthèse paraît finalement impossible entre les sensibilités propres à chaque pays mais aussi les intérêts particuliers caressés par eux.

387. En décembre 2012, s'est tenue à Dubaï la Conférence mondiale des télécommunications internationales (organisée par l'Union internationale des télécommunications, un organisme dépendant de l'ONU). À l'évidence, les positions divergeaient fortement ; sauf peut-être sur la question de résister face à l'hégémonie des Etats-Unis. Sur ce point-là, les différents Etats entendent faire entendre leur voix, même cacophonique. Ils défendent l'idée d'une multilatéralisation de la gouvernance de l'Internet.

388. La Chine fut très présente dans ce débat. Ne serait-ce, d'ailleurs, que par son poids démographique, économique et technologique. En réalité, on peut - de plus en plus - se demander si la gouvernance de l'Internet, loin d'être unique, n'est pas une tentative d'harmoniser plusieurs gouvernances simultanées. Et ce, non seulement en raison des divergences de vues entre Etats, mais encore à cause de la complexité des sujets et des enjeux (qui ne se laissent pas enfermer en une orientation souhaitable, clairement définie et univoque).

389. Il faut, par ailleurs, noter que la question de l'Intelligence Artificielle (qui est voisine, mais non exactement identique) va se poser - elle aussi - de plus en plus fréquemment, sous différents aspects. On a le sentiment d'une impasse.

Il est indispensable d'unifier la gouvernance. Faute de quoi on favoriserait la balkanisation du monde. Toutefois, cette gouvernance ne peut exister qu'en mobilisant le plus possible le multilatéralisme. Ce qui rend d'autant plus complexe son unification. C'est un peu " le serpent qui se mord la queue ". Les rivalités et alliances classiques entre Etats supposaient que seuls quelques puissants (en tous les cas des Etats se définissant comme tels) puissent à la fois engager des conflits et trouver des solutions. Ce qui fait courir un risque réel d'extension d'un conflit - faisant tâche d'huile, comme dans le cas de la Première Guerre Mondiale.

Désormais, les attaques comme les ententes peuvent se situer à toutes les échelles, sur tous les points, et en fonction des configurations les plus diverses[327]. Chacun, quelle que soit la place - modeste soit-elle - qu'il occuperait dans les hiérarchies (grâce aux ressources des connexions numériques) se verra investi d'un pouvoir considérable. Ceci, de façon souvent imprévisible; donc fort difficile à conjurer.

390. On peut craindre une sorte de guerre " hors limite ", dans laquelle même les plus puissants ne seront pas plus protégés que leurs opposants d'apparence insignifiante. Face à cette situation, le droit international semble curieusement à court d'idées. Désormais, tous les réseaux connectés - d'une façon ou d'une autre - à l'Internet, par les fibres optiques, participent de cet immense cyberespace ; lieu de tous les possibles. Les acteurs aussi bien étatiques qu'individuels disposent d'ores et déjà d'une marge de manœuvre considérable. On peut à certains égards parler d'une véritable guerre civile[328]. En tous les cas, d'une épée de Damoclès

b. La surpuissance américaine[329]

390. Ce n'est un secret pour personne, les Etats-Unis occupent une place exceptionnelle. Cela peut trouver à s'expliquer par des raisons historiques plus anciennes, mais également parce que différents acteurs américains ont tenu un grand rôle dans le processus de développement d'internet dans le monde[330].

391. Ce leadership américain se vérifie de deux façons, peut-être paradoxales. D'une part, l'Amérique se surpasse - bel et bien - dans la promotion de normes permettant de réduire les risques numériques. D'autre part, la domination américaine s'accompagne aussi d'une militarisation précoce du cyberespace. En raison de la place singulière qu'occupe ce géant politique dans le monde. Du point de vue de l'histoire du temps présent, il est certains qu'on a observé de forts déplacements d'accent, entre l'époque de Barack Obama et celle de Donald Trump. Il est certain que sous la Présidence Obama avaient été mis en valeur l'innovation et

[327] Pour une perspective d'ensemble sur cette nouvelle discipline que l'on appelle désormais la géographie des conflits : Philippe BOULANGER, *Géographie militaire et géostratégie, enjeux et crises du monde contemporain,* Paris, Armand Colin, collection U., 2011.
[328] Paul JORION, *La guerre civile numérique*, Paris, Textuel, 2011. Cf. aussi Nicolas ARPAGIAN, *La cyberguerre : La guerre numérique a commencé,* Paris, Vuibert, 2009
[329] Frédérick DOUZET et Stéphane TAILLAT, « L'affirmation du leadership américain » in collectif, *La cyberdéfense. Politique de l'espace numérique,* Paris, Armand Colin, 2018, 111-122.
[330] Thomas RID*, Rise of the Machines. A Cybernetic History,* Londres, W.W Norton, 2017.

l'écosystème numérique. Tandis qu'avec l'élection de Trump régna le sentiment à la fois d'un protectionnisme assumé et d'un rapport de forces entretenu.

392. Régulièrement des rumeurs circulent et des inquiétudes se propagent par exemple sur une utilisation de l'Internet par les Etats-Unis à des fins d'ingérence et de déstabilisation. En riposte, la Russie et la Chine tentent de faire contre-poids. Notamment, en imposant la localisation physique des données de leurs citoyens sur leur territoire. L'Europe se montre également critique à l'égard du monopole des entreprises américaines. Cela ne plut guère à l'administration américaine qui laissa entendre qu'elle pourrait favoriser une balkanisation de l'Internet. Ce qui serait, d'une certaine manière, la négation-même du cyberespace. En effet, un tel recul marquerait une rupture avec un Internet libre, ouvert et protégé à la fois. Cela irait peut-être même à l'encontre d'un esprit démocratique, que l'on associe quelquefois à l'Internet[331].

393. Il faut reconnaître aux Etats-Unis le mérite d'avoir cultivé - précocement et brillamment - une approche militaire et stratégique du cyberespace[332]. Ce grand pays, qui est un fin stratège a mesuré l'opportunité exceptionnelle que pouvaient offrir les nouvelles technologies, notamment en matière d'information. Il remarqua l'avantage asymétrique que cela pourrait leur apporter dans des conflits, il y a environ une trentaine d'années. Cependant, ils prennent également conscience de la vulnérabilité américaine ; qui serait, selon certains, " un géant aux pieds d'argile ". A partir de l'an 2000, on assiste à un tournant dans la mesure où les Etats-Unis cultivent de plus en plus le cyberespace comme un espace de bataille[333].

394. On assiste à un effort porté sur des compétences technologiques de plus en plus sophistiquées, ainsi que sur des prouesses en la matière. De sorte que les menaces et les opportunités soient évaluées en permanence. Suite à l'épisode tragique du 11 septembre, la défense et la sécurité deviennent prioritaires. On assiste à une concentration et à une coordination des ressources américaines en hommes, armes et argent.

395. La perspective demeure toujours opérationnelle. On sait que l'utilisation d'armes numériques est envisagée, dès 2003, dans la guerre contre l'Irak de Saddam Hussein. En fait, il faut attendre

---

[331] Amaël CATTARUZZA, Didier DANET, Arthur LAUDRAIN et Stéphane TAILLAT, « Sovereignty in Cyberspace. Balkanisation or Democratization », *IEE, International Conference on Cyber Conflicts,* New York, 2016, 146-154.

[332] Thomas RID et Marc HECKER, *War 2.0 : Irregular Warfare in the Information Age*, Santa Barbara, 2009, Praeger.

[333] William J. LYNN, « Defending a New Domain : The Pentagon's Cyberstrategy » in *Foreign Affairs,* 89, 2010, 5, 89-97.

la campagne de 2007–2008 contre les groupes d'Al-Qaïda à Bagdad pour constater un véritable recours ciblé aux armes numériques ; en particulier au travers de l'interception et du brouillage des communications[334]. L'Amérique fait donc preuve d'un réel activisme dans le cyberespace. Ce qui n'est pas sans poser de problèmes au niveau international, aux yeux de nombreux pays, dont sans doute les Emirats-Arabes-Unis. Ainsi, les agences américaines en charge des opérations numériques ont maximisé les qualités de leurs grandes ressources techniques, financières et les compétences de leurs ressources humaines. Honneur leur en soit rendu. Ils ont ainsi conduit avec succès plusieurs opérations.

396. Cependant, le leadership américain entretient une tension et un risque d'escalade. Les menaces de représailles - en cas d'attaques - que brandissent volontiers les Etats-Unis détériorent un climat déjà tendu. Tout est fait pour manifester la forte détermination américaine. Néanmoins, ceci contribue à transformer le cyberespace en un espace de forte conflictualité potentielle ; plutôt qu'en un espace d'harmonisation, d'échange, de pacification, et de recherche sereine de points d'équilibre.

397. L'Amérique s'en prend violemment à ceux qu'elle accuse de l'attaquer ou de la menacer. Nonobstant, il est aussi probable, du moins selon certains experts, qu'elle se livre à des vindictes cachées, à des réponses clandestines[335].

398. L'image irénique d'un cyberspace neutre, au-dessus des divisions, des tensions et des conflits du monde réel s'est largement dissipée. Un simple exemple peut-être singulièrement révélateur, celui des câbles sous-marins, qui assurent le transport des données[336]. On sait quelle est leur importance. La coupure de l'un d'entre eux peut faire tomber un pays entier dans le noir numérique. Cela a d'ailleurs été le cas de l'Algérie en 2015. Evidemment, les informations que véhiculent les câbles peuvent être surveillées et détournées. Ce qui favorise un espionnage de masse. De simples soupçons peuvent entraîner des tensions entre pays (comme cela a été le cas entre la Russie et les Etats-Unis, en 2015, suite à la présence près de câbles sous-marins d'un bâtiment océanographique le *Yantar*).

---

[334] Shane HARRIS*, @War. The Rise of Cyber Walfare*, Londres, Headline Publishing, 2014.

[335] Michael POZNANSKY et Evan PERKOSKY, « Did the US 'Hack Back' at Russia ? Here is Why it Matters in Cyberwarfare » in *Monkey Cage*, 2018, *https://books.google.fr/books?id=YHBiDwAAQBAJ&pg=PT222&lpg=PT222&dq=Poznansky+et+Perkosky&source=bl&ots=ze4CTOTy4L&sig=ACfU3U1OkoInvbDOkCXLkc8D0OkKE0K4RQ&hl=fr&sa=X&ved=2ahUKEwiFkYrm9e3pAhWRC2MBHfGqAK8Q6AEwAHoECAoQAQ#v=onepage&q=Poznansky%20et%20Perkosky&f=false*

[336] Camille MOREL, « Les câbles sous-marins : un bien commun :mondial ? » in *Etudes*, 2017, 3, 19-28.

399. Les enjeux géopolitiques s'avèrent énormes. Il faut savoir que l'immense majorité - sinon la quasi-totalité - des échanges de données entre l'Europe et l'Asie se fait par les Etats-Unis. Ce qui leur confère un leadership potentiel énorme. Cela tient aussi, sans doute, à la plus haute qualité du matériel américain. Aujourd'hui, certains pays tentent d'échapper à ce leadership américain (en le contournant par des routes alternatives), mais c'est tout sauf simple d'un point de vue logistique. On peut citer l'exemple du réseau câblier terrestre *TEA* (Transit Europe-Asie) qui place la Russie au centre des flux. Ce qui entame l'hégémonie américaine au bénéfice d'un puissant rival.

400. La Russie, nous l'avons déjà dit, entend bien mettre en place son propre cyberespace ; au sein duquel elle peut inscrire sa politique de puissance, notamment face aux géants américains et chinois. Il faut savoir qu'elle est l'un des seuls pays du monde à disposer d'un écosystème presque complet de plateformes et de services digitaux à destination des russophones. On parle du Runet pour désigner ce nouveau réseau, puissant et volontariste. D'un point de vue stratégique, c'est un atout considérable pour le pays[337].

401. La Chine, quant à elle, ne cesse de multiplier des plans, des projets, et des initiatives. À l'évidence, elle vise un leadership mondial dans dix ans. Il faut dire qu'elle possède un atout intéressant, en comparaison des puissances occidentales et même de l'Union européenne. En effet, elle n'a aucun scrupule à collecter les données de ses internautes. De plus, ses citoyens lui cèdent - en général sans réticence - une foultitude de données. Ce qui bien entendu profite beaucoup au système numérique de surveillance chinois. À l'avenir, deux scénarii sont peut-être envisageables. Selon le premier, la Chine rattrape vite les Etats-Unis et domine la gouvernance de l'Intelligence Artificielle, mais au risque d'un conflit mondial (consommé ou, au moins, latent).

402. Heureusement, il existe un deuxième scénario. La Chine est un géant, mais " aux pieds d'argile ". Cette friabilité tient justement à sa puissance. De sorte que certains problèmes internes la dissuaderont d'ambitions mondiales déraisonnables. Bien entendu, nul ne pourra ignorer sa puissance internationale, mais elle restera circonscrite. Cela limitera ses volontés d'extension mondiale.

403. Nous ne pouvons ici ? dans le cadre de notre sujet ? aller plus loin dans l'analyse et encore moins dans la prospective. L'important à retenir, cependant, est que toute législation nationale

[337] Kévin LIMONIER, « Des cyberespaces souverains ? Le cas de la Russie », in collectif, *La cyberdéfense* (op. cit), 123-129.

(y compris celle des Emirats), toute stratégie politique nationale, devra nécessairement tenir compte de ce contexte. Elle ne pourra aucunement se définir seulement *ad intra*. Pour pertinents et sages que puissent être ses choix. Définir et préciser la réponse des Emirats à la révolution numérique, ce sera aussi se confronter à la réalité du monde de demain, avec des géants, peut-être affaiblis, ou - au contraire - plus dominateurs que jamais.

c. Révolution numérique et nouvelles menaces.

404. Il y a un peu plus de sept décennies, la bombe atomique a modifié l'idée-même de la guerre ; en raison des conséquences induites ; rendant aussi improbable qu'apocalyptique un conflit mondial ouvert.

405. La dissuasion est donc devenue l'arme par excellence. Elle est risquée, mais à moindre coût humain. La révolution numérique pourrait nous faire entrer dans une autre période de l'histoire. Même si l'ampleur d'un tel risque est diversement évaluée[338]. Certes, les attaques pourraient être plus virtuelles que réelles. On ne saurait imaginer un retour à une guerre du type de celle de 14 / 18, dans des tranchées. Encore que l'improbable n'est jamais impossible. Dans la mesure où l'ampleur et le caractère imprévisible et incontrôlable d'une guerre numérique pourrait inciter – qui sait ? – à se rabattre sur des moyens de s'affronter plus classiques. Néanmoins, le fait qu'une attaque puisse venir de partout et sous des formes très diverses et inattendues crée un climat hautement anxiogène[339]. D'autant plus que de nouvelles raisons de susciter un conflit sont en train d'émerger : dans le cadre d'une compétition économique de plus en plus acharnée, qui va bien au-delà des rivalités territoriales. Celles-ci semblent presque anodines à côté.

406. Ceci dit, d'anciens motifs de conflit peuvent toujours resurgir ; y compris la susceptibilité offensée, ou l'intégrisme religieux - qui n'est hélas pas mort. Ce qui laisse augurer des risques graves pour le futur, et une atmosphère de grande incertitude et de très haute tension. Ceci, sans même parler de nouveaux chocs intracommunautaires ou ethniques qui pourraient surgir. Ainsi, ce ne seront plus seulement de nouveaux motifs de conflits qui risquent d'apparaître, mais encore - et surtout -de nouvelles formes de conflits, souvent larvés ou inattendus (à survenue immédiate, ou à explosion différée).

---

[338] Brandon VALERIANO et Ryan MANESS, *Cyber War vs Cyber Realities : Cyber Conflict in the International System*, New York, Oxford University Press, 2015.

[339] Gregory CONTI et Raymond DAVID, *On Cyber: Towards an Operational Art for Cyber Conflict*. New York, Kopidion Press, 2017.

407. Très vite, l'ensemble du fonctionnement d'un pays risque de se trouver paralysé, avec des conséquences rapides. Il s'agit d'un retour à une stratégie offensive ; au-delà de la dissuasion et de la défense. Ces deux tactiques risquent toujours d'être prises en défaut par une nouvelle astuce d'attaque. Un rapport laisse entrevoir ce que pourrait être une telle conflictualité des temps futurs. Selon le rapport « la guerre *off-limits* » des colonels chinois Quao Liang et Wang Xiangsui, l'empire du milieu est manifestement en avance en matière de développement numérique.

408. Une bonne stratégie pourrait permettre - plus que jamais - de battre un pays technologiquement plus avancé, par des moyens très divers et des attaques latérales, un peu comme une partie d'échec ou de jeu de go[340]. Une traduction anglaise de ce document est disponible sur l'Internet depuis 1999. Aux Etats Unis, l'Académie Navale le fait étudier, consciente de son importance. Une traduction française existe depuis 2003[341].

409. Le rapport propose un nouvel art de la guerre, plus global. On pourrait dire holiste. En ce sens, les nouvelles formes de guerre risquent de prolonger et d'étendre des menaces déjà actuelles. Le rapport montre qu'il est possible d'écraser très rapidement un adversaire, même sans entrer dans un conflit militaire direct, par des méthodes subtiles et discrètes (mais beaucoup plus puissantes) : en particulier par l'attaque ciblée et sournoise, de sites et de réseaux Interne. L'enjeu va être celui d'une bonne connaissance, et surtout d'une bonne maîtrise de l'intelligence artificielle.

    Dans un même ordre d'idées, le terrorisme devrait connaître de nombreux développements, à très large échelle. Le terrorisme vise à obtenir un effet immédiat, celui d'installer de façon élargie un climat d'insécurité et de peur. Rappelons que son terrain est – au moins dans l'état actuel des moyens dont il peut disposer – davantage psychologique que concret. Un petit nombre de terroristes pourrait bien mettre en péril l'équilibre entier de la planète. L'impact psychologique de toute entreprise terroriste, même limitée, est considérable et dévastateur. D'ores et déjà, des individus ou des groupes peuvent utiliser l'anonymat permis par l'espace internet pour menacer et répandre de fausses nouvelles.

410. Ce qu'on appelle " le cyberterrorisme " consiste en une sorte d'utilisation perverse et préméditée des atouts du numérique, pour faire peur, exercer des pressions, voire du chantage.

---

[340] La référence au jeu de go me semble singulièrement pertinente dans la mesure où un ordinateur où l'intelligence artificielle de Google est parvenu à apprendre le jeu de Go et à écraser la machine qui a détrôné l'homme. Cf *: https://www.huffingtonpost.fr/2017/10/18/en-3-jours-lintelligence-artificielle-de-google-a-appris-le-jeu-de-go-et-ecrase-la-machine-qui-a-detrone-lhomme_a_23247579/*

[341] *http://pourconvaincre.blogspot.fr/2009/08/la-guerre-hors-limites.html*

Il ne faut pas négliger l'impact émotionnel du numérique, parfois associé à une vulnérabilité psychologique de l'utilisateur ; notamment lorsqu'il fait un usage anxieux ou compulsif des nouvelles technologies. Le cyberterrorisme ne réside pas seulement dans la dissémination de menaces, de fausses ou vraies nouvelles inquiétantes, mais inclut également des attaques ciblées contre les réseaux, les systèmes informatiques et de télécommunications. Nous en reparlerons abondamment plus loin.

411. L'intérêt inquiet, mais néanmoins souvent fasciné du public pour le cyberterrorisme, commence dans les années 1980. Il est lié parfois à la guerre froide (menaçant de se réchauffer) ; et, dans une perspective plus irrationnelle, à l'approche d'un nouveau millénaire, de l'année 2000. D'aucuns annonçaient un *bug* aux conséquences tragiques et démesurées. Le traumatisme créé par les événements du 11 septembre 2001 entretient la hantise du cyberterrorisme. Des auteurs commencent à poser la question des risques d'une monstrueuse cyber-attaque, dans une perspective de vulgarisation, comme Winn Schwartau[342]. De façon plus fouillée, des chercheurs comme John Arquilla établissent combien les défenses actuelles (y compris celles des Etats-Unis) seraient en fait prises de court par le cyberterrorisme[343]. Pour rendre la menace plus tangible, il est peut-être judicieux de donner des exemples. Un accès illégal aux ordinateurs d'une station de recherche antarctique a fait peser un grave danger sur la vie de 58 scientifiques ; même si, fort heureusement, les futurs criminels ont été empêchés temps d'agir.

412. Plus récemment, en mai 2007, l'Estonie subi une attaque massive en raison de la destruction d'un monument commémoratif de la Seconde Guerre mondiale dans le centre-ville de Tallin, par déni de services, sous la forme d'un bombardement de demandes adressées à certains sites pour les conduire à la fermeture. Presque tous les réseaux gouvernementaux estoniens ont été victimes de cette attaque, ainsi que deux réseaux bancaires très importants.

    En octobre 2007, c'est le le site du président ukrainien Viktor Iouchtchenko, qui a été pris pour cibles par des hackers. En l'occurrence, c'étaient de jeunes nationalistes russes, sans grands moyens qui en étaient à l'origine. Ce qui donne le frisson quant à la possibilité aisée d'attaques par n'importe qui ou presque.

413. Passons sur des attaques sans vraie finalité de destruction ou de perturbation, par de jeunes chercheurs et techniciens, surtout soucieux de s'entraîner. En juillet 2009, plusieurs cyber-

[342] Winn SCHWARTAU*, Internet and Computer Ethics for Kids*, Paperback, 2001.
[343] John ARQUILLA, *Information Strategy and Warfare*, Routledge, Contemporary Security Studies, 2007.
Déjà : *Networks and Netwars: The Future of Terror, Crime, and Militancy*, New York, Rand, 2001.

attaques ont été lancées avec virulence contre les sites Web du Gouvernement américain, tels que le Pentagone et la Maison-Blanche. Celles-ci seraient imputables à la Corée du Nord.

Si les œuvres de fiction imaginent des scénarios beaucoup plus effrayants (comme dans le cas de la saga *Terminator* de James Cameron), on peut vraiment se demander si la réalité ne va pas bientôt rejoindre la fiction ; voire peut-être la dépasser. Les enjeux sont considérables et effrayants[344].

414. La menace informatique pourrait prendre deux formes distinctes et complémentaires. La première, tient à une capacité exponentiellement renforcée de mener une attaque de masse. Ceci, grâce à des hackers qui saturent les ordinateurs de l'adversaire. Un hacker est un spécialiste doté donc d'une grande compétence technique qui connaît les moyens de contourner les protections logicielles et de déceler les failles[345].

Il existe une sorte de cercle vicieux, mais pas du point de vue du hacker : plus le système trouve le moyen de se protéger, plus les hackers parviennent à le piéger - et rapidement. En effet, les techniques de protection sont semblables - à certains égards - aux stratégies des hackers. De sorte que le perfectionnement des unes s'accompagne hélas de l'ajustement des autres. Les hackers s'améliorent donc en même temps que les protections mises en place. L'hacker se sert souvent des scripts ou des programmes qui manipulent les données ; en passant par une connexion réseau, afin d'accéder aux informations du système.

415. Les techniques de piratage sont multiples et coordonnées. Elles incluent des virus, des Chevaux de Troie, des rançongiciels ou des détournements de navigateurs, mais également des rootkits et d'autres expédients. Depuis une vingtaine d'années, les *rootkits* permettent aux pirates d'accéder aux données, sans que cela ne se remarque.

Un rootkit désigne un ou plusieurs logiciels qui mettent en œuvre diverses techniques, afin d'obtenir de façon durable l'accès à un autre ordinateur (évidemment, de façon dissimulée), en général dans une intention malveillante. Les voleurs peuvent donc agir en toute discrétion. Les *rootkits* se présentent en réalité comme des outils de malware conçus spécifiquement pour passer totalement inaperçus dans des ordinateurs infectés. Ceci, afin de permettre aux pirates de contrôler l'ordinateur ; en y installant en quelque sorte du matériel. Ils se dissimulent en

---

[344] Gabriel WEIMANN*, Terror on the Internet : the new arena, the new challenges,* Washington, United States Institute of Peace, 2006.

[345] Rayna STAMBOLIYSKA, *La face cachée d'internet : hackers, darknet...,* Paris, Larousse, 2017. Cf. aussi Eric S. RAYMOND, *Une brève histoire des hackers : http://www.linux-france.org/article/these/hackers_history/fr-a_brief_history_of_hackerdom_monoblock.html*

général dans le système d'exploitation. Ils ne peuvent donc être détectés par les logiciels anti-virus, et autres. Ainsi, ils peuvent contenir de nombreux outils malfaisants, y compris un programme de capture de mot de passe, ou encore un module pour dérober des informations tels que les identifiants bancaires en ligne. Le pirate peut se connecter à distance au compte concerné et y supprimer des éléments, ou en introduire de nouveaux. C'est évidemment leur caractère sournois qui donne son importance aux *rootkits*. Certains de ces *rootkits* sont singulièrement difficiles à identifier, et plus encore à supprimer. Pour prendre pied dans l'ordinateur, ils profitent d'une vulnérabilité du système d'exploitation, ou de celle d'une application. Il est hélas très facile aujourd'hui de devenir hacker. Même des novices en la matière peuvent rapidement parvenir à des performances. En effet des scripts prêts à l'emploi existent sur l'Internet !

416. À partir de ces modèles, des hackers plus exercés parviennent à créer de nouvelles techniques de piratage. Bien entendu, les motivations d'un hacker peuvent être les plus variées. Parfois, pour désigner des pirates aux mauvaises intentions, on préfère parler de « *crackers* » que de hackers, mais ce n'est pas systématique.

    Certains *crackers* peuvent agir pour leur compte propre, ou, au contraire, parce qu'ils sont employés par d'autres, y compris des institutions. Quelquefois, selon le mode d'action déployé, on présente les différents hackers en plusieurs catégories nommées « chapeaux » : comme les chapeaux blancs ou les chapeaux noirs. Les « chapeaux noirs » sont bien entendu les délinquants animés de fort mauvaises intentions. Il y aussi les " chapeaux gris " qui agissent de manière illégale, mais sans être véritablement mus par des intentions mauvaises. Certains hackers sont parvenus à la notoriété, comme Islam Brahimi qui parvint à accéder à plusieurs ordinateurs par l'Internet au travers d'un vaste réseau. Ou encore Jon Ellch adoptant le pseudonyme de Johnny Cash, célèbre crooner américain, et qui mit en évidence la vulnérabilité des pilotes Wifi. L'Algérien Hamza Bendelladj est soupçonné d'avoir détourné dix à vingt millions de dollars de nombreuses institutions financières américaines et européennes. Le plus inquiétant est qu'il semble difficile de poser des limites aux ravages futurs d'un hacker très doué, avec des conséquences considérables.

417. La seconde, relève de ce que l'on appelle le « Cheval de Troie », en référence à l'Iliade d'Homère : à ce gigantesque cheval, construit à l'initiative d'Ulysse, pour pénétrer dans la ville de Troie (ou Illion). Il s'agit - ni plus ni plus moins - d'introduire des flux d'information, afin

de susciter l'affolement des méthodes et techniques et de la prendre en défaut[346]. Le concept de « cheval de Troie » remonte aux années 1970 et a été introduit par Daniel J. Edwards[347], avant d'être adopté par la US Air Force, et d'être popularisé par Ken Thompson[348]. La dangerosité du Cheval tient, en bonne part, à son apparence inoffensive de prime abord. Ce programme parait anodin, mais en réalité ne l'est pas. En effet, il en contient un autre, comme une valise piégée à double fond. Ainsi, l'utilisateur introduit-il dans son propre ordinateur un programme déguisé.

418. L'intrus néfaste s'appelle une « charge utile » et peut être de nature variée. Par exemple, il peut s'agir d'un virus ou d'un logiciel espion. Ainsi, le cheval de Troie se présente vraiment comme le véhicule qui fait " entrer le loup dans la bergerie ". Il est inoffensif en soi. Donc il endort la vigilance et fait entrer le programme malveillant. Les Chevaux de Troie viennent souvent de sites non officiels ou des plateformes peu sûres.

    On peut rapprocher du cheval de Troie l'injecteur ou le *dropper.* Il s'agit quant à lui d'un programme spécialement conçu en vue de propager des parasites. Le Cheval de Troie, dans son sens le plus strict, est simplement une version modifiée d'un programme déjà existant. On peut aussi évoquer la *backdoor*. Elle correspond à un programme qui va créer sur l'ordinateur une faille (autrement dit, une "porte de derrière") qui ne véhicule pas en soi le parasite néfaste, contrairement au cheval de Troie, mais va lui ouvrir l'accès.

419. Il faut aussi mesurer toute l'étendue des risques du *Remote administration tool* (RAT), à savoir des logiciels de prise de contrôle à distance d'un ordinateur. Il s'appuie sur un mécanisme souvent bénéfique, surtout lorsqu'il permet un dépannage à distance par exemple.

    De format acceptable lorsqu'ils restent encore compressés, ils deviennent au contraire envahissants une fois décompressés. On parle quelquefois de bombes de décompression. Il ne faut pas les confondre avec des Chevaux de Troie, car elles n'introduisent pas un ennemi destructeur ; mais l'effet est voisin. Ceci, dans la mesure où elles saturent l'ordinateur et ainsi le sabotent.

420. Les antivirus limitent les dégâts, mais n'empêchent pas toute attaque. En effet, le système d'exploitation peut toujours présenter des failles. La complexité et le caractère évolutif (et imprévisible) de ces attaques imposent certainement de bien développer l'arsenal législatif de

---

[346] Paul A. KARGER et Roger R.SCHELL, « Thirty Years Later: Lessons from the Multics Security Evaluation. », in
Annual Computer Security Academical Conferences, 2002, 119-126.
[347] Daniel J. EDWARDS*, Oral history. Interview*, New York, Charles Babbage Institut, 2013.
[348] Ken THOMPSON, *A brief introduction : http://www.linfo.org/thompson.html*

prévention et de combat. Même s'il risque d'être toujours en retard sur de nouvelles techniques mises en place.

Le plus grave dans tout cela est l'absence de règle, la violation de toute réglementation des conflits, en ce qui concerne les attaques dont les formes ne sont pas encore connues. Tout ce qui n'est pas interdit de façon explicite est considéré comme légal. On devine les conséquences à large échelle.

421. Les formes d'intrusion semblent multiples et imparables. Dès lors qu'une attaque sera déjouée, une autre inattendue - toute nouvelle - pourra être lancée. Jusqu'alors, la guerre ne connaissait qu'un nombre limité de scénarii possibles. Tout outil informatique pourra servir au combat, afin d'entretenir le conflit. L'espionnage prendra des proportions gigantesques. Il ne sera plus possible de le conjurer en colmatant une faille. Une autre faille pourra être ouverte, plus redoutable encore.

422. L'Occident semble effrayé par cette perspective. Ce que l'on peut comprendre. Il est assez lent à concevoir de nouvelles parades de défense. La protection actuelle face à la sophistication accélérée des techniques d'attaques rend vaine la sensation d'être à l'abri. Désormais l'interruption et la neutralisation de l'ensemble des transmissions se présentent comme une menace constante.

Une nouvelle idéologie du combat est en train de poindre. Elle ne peut que séduire les terroristes. Elle se base sur une stratégie cherchant en l'occurrence la recherche immédiate du coup létal ; visant à mettre hors d'état de nuire (de façon globale) l'adversaire. La rupture est évidente avec les guerres anciennes. Elles se caractérisaient par une série d'attaques et de victoire donnaient l'avantage à l'un ou l'autre. L'un comme l'autre des adversaires pouvaient perdre, puis retrouver l'avantage. Elles ne visaient pas l'élimination totale de l'autre, mais un meilleur positionnement, parfois provisoire, en vue d'une victoire encore à venir.

La phrase célèbre du Général de Gaulle appelant en 1940 les Français à mener la lutte en constitue l'expression la plus parfaite et la plus suggestive : « la France a perdu une bataille mais elle n'a pas perdu la guerre ». Désormais, perdre une bataille pourrait bien être perdre nécessairement la guerre. Par exemple, la coupure immédiate de câbles sous-marins pourrait en

un instant déconnecter de grands espaces. D'ores et déjà, selon une formulation très juste, les cyberattaques constituent une arme de guerre en temps de paix[349].

Ainsi, la guerre va totalement changer de nature. Certains parlent quelquefois "de l'âge ou de l'ère du Verseau". Sans mauvais jeux de mots, nous entrons manifestement dans l'âge des réseaux en matière de défense[350]. Le monde entier devient un espace de puissance interconnecté. Ceci, au travers de réseaux aussi bien verticaux (plus faciles à identifier et moins souples) qu'horizontaux (plus nombreux et de plus en plus incontrôlables).

423. Les initiatives lancées, évidemment de façon inattendues et très rapides, viseront par exemple à voler des données, comme le font les services secrets militaires ou diplomatiques ; mais aussi les données personnelles détenues par les Banques ; mais aussi à endommager gravement - de préférence détruire complètement - les systèmes d'information, dans une forme de « vandalisme virtuel »[351] ou de « vandalisme cybernétique »[352] souvent très radicale.

424. L'un des spécialistes de la question, Nicolas Ténèze[353], ne recense pas moins de douze catégories d'attaques dans la cyber sphère, qu'il est intéressant d'énumérer : la neutralisation d'un système informatique pour le rendre inopérant ; le cyber espionnage ; le cyberharcèlement ; la cyberfraude (par exemple aux examens, lors de votes, ou dans l'imitation frelatée de documents officiels) ; le *cyber-whistleblowing* (le fait de sonner l'alarme et de créer la panique) ; la cybercontrefaçon et le cybermarché noir ; la cyberfinance criminelle ; la cyberpropagande ; la cyber usurpation d'identité ; le cybercambriolage ; et, enfin, le *défacing* de site dénaturant sa page d'accueil.

425. On se souvient que le 21 avril 2009, le *Wall Street Journal* avait révélé que des hackers avaient réussi à pénétrer dans les réseaux protégés de l'administration américaine, pour y dérober avec succès des centaines de téraoctets d'informations ultraconfidentielles concernant le chasseur américain F-35. Cette information a fait l'effet d'une bombe dans la presse et créé un véritable choc psychologique. On estimait - à tort ou à raison - que ces talentueux hackers étaient d'origine chinoise.

---

[349] Dominique MONGIN, *Les cyberattaques, armes de guerre en temps de paix* : *https://www.cairn.info/resume.php?download=1&ID_ARTICLE=ESPRI_1301_0032*
[350] Joseph HENROTIN*, L'art de la guerre à l'âge des réseaux*, Paris, ISTE, 2017.
[351] Stéphane LEMAN-LANGLOIS*, La sociocriminologie*, Montréal, Presses Universitaires de Montréal, 2007.
[352] Olivier DANINO*, https://www.cairn.info/revue-securite-globale-2013-2-p-15.htm*
[353] Nicolas TENEZE, *Combattre les cyberagrassions*, Paris, Nuvis, 2017.

426. L'un des autres exemples d'attaque est celui de la centrale nucléaire de Bouchehr en Iran, en 2010, peut-être par Israël et les Etats Unis. Elle avait permis de neutraliser un objectif sans faire de victimes humaines, grâce à un virus hautement sophistiqué du nom de Stuxnet[354]. Celui-ci était parvenu à dérégler le contrôle des automatismes, des robots, et de la distribution d'électricité, en passant inaperçu pendant des mois. Il s'agit d'un ver informatique, découvert en 2010, qui aurait été créé par la NSA, afin de s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium, peut-être à la demande des administrations Bush et Obama. Il s'insère dans une vaste opération dont le nom est Olympic Games. Sa complexité et son efficacité sont tout-à-fait remarquables. De sorte qu'il s'avère capable d'espionner et de reprogrammer des systèmes industriels, tout en camouflant les modifications introduites.

427. Il aurait gangréné 45 000 systèmes informatiques, dont 30 000 situés en Iran, y compris des PC appartenant à des employés de la centrale nucléaire de Bouchehr. Les 15 000 autres systèmes informatiques touchés seraient des ordinateurs et des centrales situés en Allemagne, en France, en Inde et en Indonésie, tous liés à Siemens. Ce ver très pernicieux s'introduirait, en particulier grâce à des clés USB infectées, et utiliserait ensuite des mots de passe. L'hypothèse la plus probable est qu'il s'agit d'une attaque menée conjointement par les Etats-Unis et Israël. Du reste, un général israélien a reconnu être le responsable de cette attaque, Gabi Ashkenazi. La subtilité, mais également l'ampleur potentielle d'une telle attaque, en font un véritable événement historique.

428. L'année suivante, en 2011, plusieurs centaines de comptes Gmail appartenant notamment à de hauts fonctionnaires américains, mais aussi à des dissidents chinois, à des militaires de haut rang ainsi qu'à des journalistes ont été piratés ; peut-être par la Chine, qui a démenti. De très nombreux autres exemples pourraient être cités. Ainsi, en février 2016, la Banque centrale du Bangladesh fut victime d'un piratage informatique (associé au vol de plus de 81 millions de dollars). Les 12 et 13 mai 2017, une cyberattaque de grande ampleur s'en prend de manière très efficace aux ordinateurs de multinationales et de services publics d'une centaine de pays : aussi bien des hôpitaux britanniques, que des multinationales comme Renault, ou encore le ministère russe de l'Intérieur.

[354] Kim ZETTER, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Londres, Crown Publishing Group, 2014

429. Il va de soi que ce nouveau contexte exige de nombreux investissements, dans un esprit de perpétuel renouvellement. Il convient - de prime abord - d'inventorier les secteurs les plus stratégiques (les objectifs aussi bien civils que militaires), de même que les risques de paralysation immédiate d'un vaste secteur d'activités.

Il est ensuite important de bien maîtriser les techniques d'intrusion des infrastructures informatiques. Cela permettra d'anticiper les nouvelles formes qui peuvent apparaître d'un jour à l'autre - et frapper comme la foudre en plein ciel. La plus haute compétence technique doit se doubler de la vigilance de chaque instant.

430. Il faut savoir que des réseaux dormants[355] peuvent, à chaque instant, être réveillés. Cela implique naturellement la mise en place de la cyberdéfense. Il convient de prendre acte de la rapidité avec laquelle de nouvelles attaques sont conçues. Des secteurs particulièrement sensibles doivent faire l'objet d'une attention prioritaire : il s'agit de la surveillance des processus industriels, du transport des produits chimiques, de l'approvisionnement des villes en eau, de la commande et de la gestion de l'énergie électrique, des canalisations de gaz et de pétrole, des sites où se déploie la recherche de pointe.

431. La cyberdéfense regroupe l'ensemble des moyens qu'il est possible de mettre en œuvre pour faire face aux attaques dans le cyberespace : soit de manière préventive, soit pour en limiter les dégâts, soit pour les vaincre après coup. Nicolas Ténèze discerne en son sein, la cyber sureté, la cybersécurité, la cyber-résilience et la cyber-agression (la meilleure défense étant souvent l'attaque). Ce sont des concepts sur lesquels il nous faudra revenir un peu plus loin à cause de leurs implications juridiques. L'enjeu est considérable. À l'échelle de la planète, le marché pourrait s'élever à 100 milliards de dollars. La cyberdéfense est au croisement des prouesses technologiques et des enjeux stratégiques et géopolitiques. Les différents réseaux informatiques qui innervent un pays sont vitaux. Ils vont du nucléaire à l'approvisionnement en eau, secteur particulièrement sensible dans les Emirats.

432. Aujourd'hui, en France par exemple, la cyberdéfense est prise en charge par l'ANSSI. Cette Agence est directement placée sous l'égide du Premier ministre. Il en va de même pour le centre d'expertise technique " DGA MI ", qui dépend du Ministère de la Défense. Un rapport publié

[355] Choukri HMEHD, *Les réseaux dormants, contingence et structure* : *https://www.cairn.info/revue-francaise-de-science-politique-2012-5-page-797.htm*

le 13 janvier 2006, sous le titre « La Sécurité des systèmes d'information »[356] , rédigé par le député Pierre Lasbordes a pointé le retard préoccupant du pays face aux impératifs de sécurité des systèmes d'information : tant au niveau de l'Etat qu'au niveau des entreprises, à de rares exceptions près.

433. L'organisation est insuffisante et dispersée. En 2008, le sénateur Roger Romani a publié un autre rapport sous le titre « Cyberdéfense : un nouvel enjeu de sécurité nationale »[357]. Il y dresse le même constat d'impréparation et de désorganisation. Toutefois, le Livre blanc sur la Défense et la Sécurité nationale de 2008 marque bel et bien un tournant. En effet, il donne toute sa place dans l'édifice de la défense de la France à la cyberdéfense, en insistant sur la mise en place d'une stratégie de défense active, sans négliger les actions offensives. En 2009 est donc créée l'ANSSI, à savoir l'Agence nationale de la sécurité des systèmes d'information, par décret du Premier ministre. Le pas en avant n'est pas négligeable.

434. Le 18 juillet 2012, le sénateur Jean Marie Bockel dépose, au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat, un nouveau rapport d'information mieux élaboré et plus encourageant. Il porte le titre « La cyberdéfense : un enjeu mondial, une priorité nationale »[358]. Cet axe devient désormais prioritaire.

Toutefois, les efforts déployés en France n'égalent pas ceux de la principale agence des Etats Unis, le Cyber Command, qui fait partie des forces armées du pays. En France, un récent rapport gouvernemental du 14 février dernier montre la prise de conscience de l'importance et de l'imminence de la menace[359]. Il propose des pistes à partager avec quatre autres pays qui lui semblent chargés de responsabilités particulières : à savoir les États-Unis, la Russie, la Chine et le Royaume-Uni. Avec lucidité, honnêteté et franchise, le rapport commence par reconnaître que la France accuse toujours un déficit en matière de sécurité numérique (lié peut-être à la pesanteur institutionnelle du fonctionnement du pays et une approche toujours trop cloisonnée et sectorielle et insuffisamment globale).

435. Parmi les sept points mis en valeur par le rapport, le septième semble revêtir une importance particulière, même s'il est peut-être plus délicat à mettre en œuvre. En l'occurrence, il s'agit de

---

[356] *ww.ladocumentationfrancaise.fr/rapports-publics/064000048/index.shtml*
[357] *https://www.senat.fr/notice-rapport/2007/r07-449-notice.html*
[358] *http://www.senat.fr/rap/r11-681/r11-681_mono.html*
[359] *http://www.lepoint.fr/high-tech-internet/comment-la-france-se-prepare-a-une-cyberattaque-14-02-2018-2194949_47.php*

multiplier les actions internationales visant à promouvoir une gouvernance collective et maîtrisée du cyberespace, face à une menace protéiforme.

Après des débuts prometteurs à l'échelle internationale en 2013 et 2015, les négociations paraissent piétiner, alors qu'il y a urgence. Des mesures de protection prises par un seul pays seraient désormais bien peu efficace dans le contexte de la connexion globale du monde. Depuis des années pourtant, la cyberguerre semble avoir commencé[360]. En France, une unité de 7.000 soldats environ (dont une bonne moitié de réservistes) est d'ores et déjà en train de se constituer, mais la menace est mondiale.

436. Cela peut expliquer le catastrophisme de certaines hypothèses prospectives, comme celles de Jacques Attali[361], sur l'avenir de notre monde. Les mondes civil et militaire deviennent totalement poreux : de sorte que le champ de bataille d'un conflit ne peut plus être circonscrit. Le budget annuel de la France en la matière est de 75 millions d'euros. C'est beaucoup plus faible que les 750 millions d'euros sur quatre ans promis par David Cameron au Royaume-Uni en 2010. Sans parler des 15 milliards de dollars d'appels d'offres lancés chaque année dans ce domaine par les départements de la défense et de la sécurité aux Etats-Unis.

La mise en place d'un arsenal juridique très précis est à mettre sur pied de façon urgente. Celui-ci constitue sans doute la priorité. Il doit concentrer notre attention de juristes. Chaque pays doit y apporter sa pierre. Cependant, l'édifice entier ne peut qu'être construit à l'échelle du monde entier. Y compris lorsque cela gêne des pays tentés par des attaques sournoises ou de l'espionnage sauvage, ou du moins accusés de le faire comme la Chine.

437. Il est surtout important de prendre conscience de l'urgence d'opposer à chaque nouvelle attaque une nouvelle technique de défense et de protection. Tout en intégrant que, dès qu'une attaque est conjurée, une autre s'élabore - plus sophistiquée et inattendue. La logique est celle d'un cercle vicieux, qui peut cependant être contrôlée par la rapidité avec laquelle la riposte et la prévention conjurent chacune des funestes entreprises[362].

438. Le moins que l'on puisse dire est que le monde qui s'annonce ne semble pas de tout repos. Une vigilance de chaque instant s'impose, sur le mode d'une gestion à flux tendu. Il faut comprendre qu'une guerre de tous les instants est en train de s'engager, qui ne laisse guère de périodes de

---

360 Nicolas ARPAGIAN*, La cyberguerre. La guerre numérique a commencé*, Paris, Vuibert, 2009.
Aussi *: https://www.cairn.info/resume.php?ID_ARTICLE=RINDU_104_0023*
361 Jacques ATTALI, *Vivement après-demain,* Paris, Fayard, 2016.
362 Daniel VENTRE*, Cyberattaque et Cyberdéfense*, Paris, Hermès Lavoisier, 2011.

répit et encore moins de trêve de Dieu, contrairement aux affrontements du Moyen Age. Il faut la conduire avec sagacité, sans relâche, et en réajustant sans cesse de nouvelles stratégies[363].

C'est le monde que la révolution numérique a fait naître, et continue à faire grandir sous nos yeux. Un retour en arrière ne semble pas concevable. À l'humanité d'être à la hauteur, sans catastrophisme inutile, mais avec lucidité. Ce qui demande la coopération de tous, mais aussi certainement une nouvelle charte éthique, et passe par la pleine valorisation, à toutes les échelles, d'instruments juridiques appropriés.

439. Notre deuxième partie va nous aider à en prendre la mesure, dans une perspective d'avenir. Après avoir - en somme - dressé une sorte d'inventaire de la situation, sous la forme du panorama, il nous faut à présent, sous un angle davantage juridique, envisager les défis à relever et les parades à envisager.

[363] Bertrand BOYER*, Cyberstratégie, l'art de la guerre numérique*, Paris, Nuvis, 2012 ; *Cybertactique : conduire la guerre numérique,* Paris, Nuvis, 2014.

PARTIE II : LA REVOLUTION NUMERIQUE MAITRISEE PAR LES EMIRATS ARABES UNIS

440. L'inventaire des défis actuels à relever doit s'articuler autour d'une prise en compte de la vocation sociétale qui est celle du droit. Le droit ne constitue pas simplement un arsenal utile pour les individus, mais plutôt un cadre dominé par le souci du bien commun, dans la volonté de protection de tous - en particulier des plus faibles. Le bien commun bien qu'essentiel s'avère complexe à réaliser. Il n'est pas forcément la somme des biens particuliers, mais il ne saurait non plus résider en une sorte d'abstraction qui ne satisferait personne ; formant une forme adoucie de totalitarisme impersonnel. Il laisse cependant entendre que le droit ne se réduit jamais à une sorte de champ de bataille permanent entre des intérêts singuliers – de personnes physiques ou morales. Il vise une sorte d'unité harmonieuse, ou du moins la plus harmonieuse possible. Chacun, d'une certaine façon, peut alors y trouver - sinon son intérêt du moins - sa place légitime et la protection élémentaire qu'il peut revendiquer.

441. Il peut et doit également y trouver un socle de garanties pour ses libertés individuelles. Cette unité harmonieuse recherchée, peut-être utopique et asymptotique il est vrai. Toutefois, il constitue un horizon, aussi bien dans les rapports entre personnes, qu'au niveau de l'administration globale[364].

442. Il importe, à titre liminaire, de souligner que, d'une part, le droit, en particulier dans la tradition française, peut être compris comme un ensemble de normes non purement arbitraires, mais qui tient compte l'homme comme tel, sa nature morale et sa destinée communautaire et non solitaire[365].

Sans revenir sur l'éventuel ancrage théologique et transcendant du droit, on ose reconnaître des droits qui seraient issus de la nature humaine ; pour malaisés qu'ils soient à définir. Ceux-ci visent à protéger la dignité, l'intégrité. On mesure bien alors la raison d'être d'une protection de la vie privée face aux nouvelles technologies. Sa violation offenserait sérieusement la dignité humaine. Cette protection doit - bien entendu - se déployer dans le cadre plus étroit de la sécurité

[364] Rémy CABRILLAC *, Introduction générale au droit*, Paris, Dalloz, 11e éd., 2011 ; Stamatios STITZIS*, Introduction à la philosophie du droit,* Paris, Vuibert, 2011.
[365] Blandine KRIEGEL, *Droit naturel et droits de l'homme,* Paris, PUF, 1989 ; Rainer Maria KIESOW, *L'unité du droit*, Paris, EHESS, 2014.

de chaque personne. Par exemple, face à des menaces personnelles comme celles d'un escroc qui va pirater un compte.

Il va également de soi qu'elle s'étend bien au-delà, dans le sens d'une protection collective. Par exemple, dans la perspective de possibles cyberattaque, face au terrorisme notamment. Le plus angoissant, mais également le plus stimulant, est de se trouver dans un contexte où la dangerosité future, de plus de plus en difficile à mesurer.

443. Il est souhaitable, d'autre part, de prendre nettement conscience que le rôle du droit se complique considérablement dans la mesure où il peut exister de vrais conflits de devoirs. Les dilemmes moraux sont multiples. Par exemple, un Etat a le droit de se protéger du terrorisme, mais jusqu'où peuvent aller les limitations de certaines libertés (par exemple le droit d'aller et venir ?).

444. Il semble donc que la tâche du juriste ne puisse se limiter à énoncer des droits intangibles et fondamentaux. Il doit envisager la complexité de situations où il faut cultiver nécessairement l'art du compromis en raison d'enjeux en concurrence, de situations d'urgence et de risques. Cela devient singulièrement complexe, lorsque les menaces relèvent du numérique et sont donc nouvelles, difficiles à circonscrire, et surtout inattendues.

445. Il faut affronter sereinement - mais lucidement - la complexité d'un futur qui peut laisser augurer une sophistication (et une ampleur bien supérieures) des agressions numériques. On ne pourra donc pas se contenter purement et simplement de déduire de droits fondamentaux une législation parfaite ; comme si la conjoncture actuelle était purement et simplement destinée à se perpétuer.

    D'une certaine façon, il faudra plutôt veiller à un certain équilibre (mais fort difficile à évaluer), à un balancement constant entre des exigences toutes importantes, comme la liberté d'expression et la sécurité.

446. Les décisions ponctuelles sont loin d'être évidentes. Elles sont toujours tâtonnantes. Cela vaut - a fortiori - des législations à organiser et à préciser aussi. Le risque peut exister alors de voir *a minima* le droit comme ce qui empêche la pire des situations, et évite des maux plus grands. Il serait alors une digue, indispensable, mais toujours imparfaite ; et surtout sans véritable effet positif. Il s'agirait donc surtout, par le droit, de construire un cadre du moindre mal possible.

447. Ce double rôle du droit se complique encore - de plus en plu -s dans le domaine que nous étudions, en raison de mutations rapides et imprévisibles. Celles-ci changent en peu et de façon radicale la donne. Elles imposent une sorte de réactivité prudente à cultiver en permanence, face à des risques inattendus et des dérives imprévisibles. Les solutions ne sont certainement pas évidentes à trouver et indiscutables. Cette incertitude à laquelle le juriste est condamné donne en même temps toute leur importance à sa recherche et à sa réflexion.

Elle se décline en quelque sorte à deux niveaux. D'abord, celui du droit privé, hanté par la nécessité de préserver la dignité humaine. Ensuite, celui du contrôle indispensable d'une nouvelle criminalité, à différentes échelles, en plein essor, urgent, actualité oblige. Qui relève du droit pénal et aussi en partie du droit international.

TITRE I : LA NÉCESSITÉ DE PRÉSERVER LA DIGNITÉ HUMAINE (Droit privé)

448. Le droit privé, différent du droit public[366], doit absolument garder le cap de la préservation de la dignité humaine. Cela est, en effet, l'une de ses vocations premières. On sait précisément qu'en droit la première distinction est celle entre le droit privé et le droit public, comme les deux premières grandes branches de la discipline.

On peut dire que les sources du droit privé (l'idée de le codifier soigneusement) remontent à la Rome antique. Par ailleurs, il est fortement centré sur le droit des personnes[367]. Celui-ci peut, à l'évidence, être menacé par l'essor technologique. En l'espèces, les droits civils ont une importance fondamentale[368]. Souvent associés à des valeurs morales, ils expriment les prérogatives attachées à la personne. On peut songer à différents droits civils, comme le droit au respect de la vie privée, de la vie familiale, du domicile et de la correspondance ; le droit à l'image ; le droit d'aller et venir ; mais aussi la liberté d'expression et de réunion.

449. Cette composition intrinsèque est relativement indépendante dans ses lignes générales du contexte et des moyens technologiques. Certains problèmes se sont posés certainement de façon plus ou moins identique tout au long de l'histoire. D'une certaine façon, du reste, ces droits constituent une sorte de socle auquel fait écho l'ensemble du dispositif juridique d'une manière ou d'une autre.

Il est bien évident que les futures mutations technologiques et numériques créent des difficultés et des défis à l'égard de ces droits. De sorte que la nouveauté incroyable de la situation ne signifie pas pour autant une réflexion juridique se tissant *ex nihilo*. À l'évidence, cette révolution conduit à une sorte de réactivation de problématiques anciennes ; traversées depuis toujours par des tensions internes ; qui ne tiennent pas seulement au contexte mais à la difficulté constante d'identifier une sorte de voie moyenne et de trouver un point d'équilibre.

450. D'anciens questionnements remontent donc à la surface. Le contrôle de la diffusion de nouvelles ne met-il pas en cause, par exemple, le droit à la liberté d'expression ?

---

366 Elisabeth ZOLLER*, Introduction au droit public*, Paris, Dalloz, 2e éd. 2013 ; Didier TRUCHET*, Le droit public,* Paris, PUF, 2014.

367 Philippe MALAURIE, *Droit des personnes : la protection des mineurs et des majeurs*, Issy-les-Moulineaux, LGDJ, 2016.

368 Christian ATLAS, Le droit civil, Paris, PUF, Que sais-je ?, 2004 ; Louis BACH*, Droit civil : introduction à l'étude du droit, les personnes physiques, la famille, les biens, les obligations, les sûretés*, tome I, 13e éd, Paris Sirey, 1998 ; Luce TOPOR*, Introduction au droit privé et au droit civil*, Paris, Les Cours de droit, 1998.

Le phénomène des *big data*, comme nous l'avons fortement souligné précédemment, ne met-il pas en danger le droit à la protection de la vie privée ? L'indiscrétion que permet et favorise notre culture de la transparence peut entrer directement en conflit avec la protection de la dignité humaine, et ses corollaires (comme la protection de la confidentialité et de la vie privée).

451. Certes d'autres menaces peuvent déjà poindre à l'horizon, à commencer par celles de la patrimonialisation du corps grâce aux nouvelles techniques. Toutefois, il nous semble que de façon plus immédiate c'est la disparition du secret légitime et de l'oubli qui constitue une dérive très grave ; même lorsqu'il ne s'agit pas de questions sensibles ou délicates, du reste.

Il nous faut donc nous pencher davantage sur les risques de cette injonction à la transparence. Ceci d'autant que les limites de celle-ci sont potentiellement infinies.

452. Non pour la considérer d'un point de vue sociologique, psychologique ou politique, mais bien plutôt pour l'affronter du point de vue juridique, de ce qui devrait être, ou de ce qu »il faut éviter qu'il advienne.

Chapitre I : Les risques de la transparence

453. Nous avons déjà évoqué les risques de la transparence, qui constitue à la fois un état de fait de plus en plus fréquent, mais également une injonction parfois très abrupte et implacable. Jusqu'à une date récente, les données n'étaient pas accessibles, ni parfois même rassemblées. Éparses, elles se prêtaient plus difficilement à l'investigation et à la possession.

Ce n'est plus le cas aujourd'hui. Il y a bien entendu beaucoup à redouter des menaces liées à une volonté de transparente, finalement totalitaire ; au-delà même de tous les risques liés à la criminalité, et aux pratiques illégales.

454. Même si ces risques nous donnent une vision de cauchemar, ils ne peuvent nous faire négliger ceux qui tiennent purement et simplement à un cadre légal insuffisamment contrôlé ; et qui permettent peut-être des atteintes à la dignité humaine en la matière. Il nous faut accorder une attention particulière aux mutations liées à l'analyse prédictive et à l'indiscrétion du numérique, par exemple des réseaux sociaux, surtout en référence au passé.

455. Le droit à l'oubli est une condition impérative pour que la personne, même coupable, puisse avoir un avenir. L'Internet-même semble en effet mettre en cause le principe, sur lequel se fonde l'idée de prescription.

Section I : La révolution de l'analyse prédictive

456. L'émergence de l'analyse prédictive[369] conduit à une situation radicalement nouvelle à bien des égards. L'analyse prédictive englobe en réalité une variété de techniques issues des statistiques, techniques permettant aisément d'extraire et d'abstraire des connaissances à partir de données et de " la théorie des jeux "[370]. On part de l'analyse des faits présents et passés.

Sans aucun doute, certains phénomènes vont en s'accentuant, comme la baisse du coût du stockage, mais aussi l'explosion du nombre de données, associés à la formation de *clouds*. Le

[369] William GREENE*, Econometric Analysis*, Londres, Prentice Hall, 7éd, 2012; Eric SIEGEL*, Predictive Analytics? Data Mining and Big Data. Myths*, *Misconceptions and Methods*, Basingstoke, Palgrave Macmillan, 2014.
Video : Olivier GRISEL, L'analyse prédictive, https://www.youtube.com/watch?v=R8QLyBXlEYg;
[370] Nicolas EBER, *Théorie des jeux*, Paris, Dunod, coll. « Les Topos », 2004 ; Ken BINMORE, *La théorie des jeux : une introduction*, Paris, Arkhè, 2015 ; Gaël GIRAUD, *La théorie des jeux*, Paris, Flammarion, coll. « Champs Essai, 2009.

juriste semble donc devoir s'interroger sur la façon dont il lui est encore possible d'affronter - pour la contrôler - l'explosion du nombre de données en circulation.

a. L'explosion du nombre de données

457. Le *cloud computing*[371] se présente comme une nouvelle technique de stockage, à distance, par l'intermédiaire d'un réseau, le plus souvent l'Internet. C'est une solution beaucoup plus commode, beaucoup plus rapide. Elle prend moins de place. Ce mode de stockage est très souple et efficace. Il exprime une amélioration considérable des systèmes informatiques. Il traduit un phénomène de délocalisation et de déréalisation. Cette déréalisation correspond - du reste - très bien avec tout le dynamisme de la révolution numérique.

458. L'émergence du *cloud* est liée à l'augmentation considérable de la puissance des serveurs. Pour les entreprises, l'avantage est considérable. Elles ne se servent plus de leurs propres serveurs, mais accèdent à des services très perfectionnés. Certes, parfois moins performants et parfaits, au moins au départ, en raison de la complexité des liaisons réseau et de la multiplicité des intervenants, mais prometteurs dans un futur proche.

459. Il paraît important de rappeler que le *cloud computing* contribue à l'émergence de tout un secteur d'activités. L'application la plus connue est celle du *iCloud d'Apple*, qui existe depuis septembre 2011. Il s'agit d'un remarquable système de sauvegarde, auquel un grand nombre de particuliers se réfère.

De plus en plus de grandes entreprises contractualisent les services de *cloud computing*. Elles misent sur leurs bienfaits dans le futur, qu'elles espèrent véritablement exponentiels.

Les contrats en question présentent un intérêt considérable pour le juriste. En particulier, par certaines de leurs clauses qui peuvent concerner la sécurité ou la confidentialité. C'est l'entreprise cliente qui est juridiquement responsable. En effet, le fournisseur, comme Apple par exemple, n'est qu'un sous-traitant.

La rédaction de tels contrats se présente comme vraiment très complexe. On note d'ailleurs que Microsoft, toujours en tête dans l'élaboration de nouveaux services, a constitué un service pour

[371] Romain HENNION, Hubert TOURNIER, Eric BOURGEOIS, *Cloud computing : Décider - Concevoir - Piloter - Améliorer*, Paris, Eyrolles, 2012 ; Guillaume PLOUIN, *Cloud Computing, Sécurité, gouvernance du SI hybride et panorama du marché*, 4e éd., Paris, Dunod, 2016 ; *Tout sur le Cloud Personnel, Travaillez, stockez, jouez et échangez... dans le nuage,* Paris, Dunod, 2013.

aider à la rédaction de semblables contrats[372]. Nous sommes à l'évidence en face d'un secteur en pleine expansion. Il devrait exploser ces prochains temps. Des incertitudes continuent à peser sur le gain futur d'un recours au *cloud computing*.

460. Du point de vue économique et financier, il y a parfois le risque que le coût total soit plus important que prévu, en particulier selon le mode d'utilisation et la durée. Une étude comparative est toujours nécessaire. Il faut éviter les arnaques. C'est pourquoi une vigilance s'impose également au sujet des coûts cachés et collatéraux.

Du point de vue juridique, il serait ainsi opportun de veiller à faire des factures très lisibles. De façon globale, on peut toutefois estimer que les avantages l'emportent largement sur les inconvénients. Sur un plan économique, si le choix est fait avec sagacité et prudence, l'adoption du *cloud computing* pourrait permettre d'économiser entre un quart et un cinquième des dépenses actuelles. Ce qui, lorsqu'il s'agit de sommes importantes, constitue une épargne conséquente. Par ailleurs, le *cloud computing,* encore à ses débuts, peut laisser augurer d'autres développements lucratifs. On peut aussi arguer qu'il ne demande aucun investissement préalable, ni en argent, ni en ressources humaines, ni en matériel. Pour autant, il y a toujours des polémiques. En particulier, lorsqu'il s'agit du secteur public. On peut, en effet, se demander si la sécurité est vraiment garantie.

461. Le fait que la connexion se fasse généralement par l'Internet constitue également un facteur de risques pour une confidentialité de plus en plus fragilisée (par le développement des techniques de cyberattaques, comme nous l'avons vu plus haut). Cela vaut certes pour les particuliers, mais surtout pour les entreprises, quelle que soit leur ampleur. Or, pour les grandes entreprises, dans le cas du stockage en interne, ce risque était jusqu'alors réduits grâce aux techniques de cloisonnement des réseaux[373]. Pour une entreprise, il peut également y avoir quelque chose de très gênant dans le fait de dépendre de la qualité du réseau externe ; la disponibilité n'étant jamais garantie de façon absolue.

462. Plus fondamentalement, du point de vue juridique, les entreprises ne sont jamais assurées - sinon par un contrat qui peut être violé ou contourné - de l'utilisation éventuelle de leurs données, entre les mains d'un tiers. Des questions spécifiques peuvent aussi se poser, en raison de l'absence de localisation précise des données du *cloud.*

---

[372] MICROSOFT*, Cloud economics, Livre blanc*, novembre 2010 [PDF] sur le net.

[373]Rapport CIGREF, *Fondamentaux du Cloud Computing : Le point de vue des Grandes Entreprises*, mars 2013 : *http://archive.wikiwix.com/cache/?url=http%3A%2F%2Fimages.cigref.fr%2FPublication%2F2012-2013-Fondamentaux-Cloud-Computing-Point-de-vue-grandes-entreprises.pdf*

463. Quelle législation nationale, ou même internationale, suivre dans un tel cas ? Par ailleurs, en regard de l'explosion de la délinquance numérique, il faut se souvenir que les services de *cloud computing* peuvent être sournoisement utilisés comme base de lancement de cyberattaques.

Ainsi, en 2009, un service du *cloud* public d'Amazon a-t-il été piraté et a-t-il pu permettre d'infecter de très nombreux ordinateurs, grâce à un Cheval de Troie.

Parmi les autres aspects négatifs du *cloud,* il y a les conséquences sur l'environnement. Ce système est très consommateur d'énergie (dans fermes de serveurs associées). De façon un peu paradoxale, on semble donc fondé à dire que si le *cloud*, comme d'autres nouveautés technologiques, fort remarquables par ailleurs, permet des pratiques simplifiées, il complexifie la réflexion juridique. Il pose des problèmes délicats et enchevêtrés en matière de sécurité et de gestion, imposant de relever de nouveaux défis, intuitivement saisis, mais bien difficiles à préciser dans l'état actuel des choses.

464. C'est un tout nouveau paradigme juridique et pratique qui semble émerger avec le *cloud*. L'étendue de cette révolution en cours est encore difficile à évaluer. De nouvelles tâches vont s'imposer, tandis que d'autres vont devenir superflues, avec pour conséquence des mutations dans la vie active et dans les professions. Tout dépend donc, en dernière instance (comme pour bien des choses) de l'usage ingénieux et habile de ce qui reste un moyen, pour sophistiquer et en partie imprévisible qu'il puisse être[374].

C'est là que le juriste a certainement son mot à dire ; et l'aura peut-être de plus en plus. La croissance exponentielle des données demeure un élément incontournable. Il se présente véritablement comme une situation totalement nouvelle. Elle oblige la législation à faire vite et bien, mais laisse aussi supposer la multiplication des techniques de stockage.

465. Il faut savoir que les coûts de traitement des données sont presque soixante fois moindres qu'il y a encore dix ans, et que le prix moyen des capteurs a lui aussi diminué de moitié. Il ne suffit cependant pas de prendre conscience de cette explosion quantitative. En effet, la simple addition de données isolées ne constituerait pas une vraie révolution. Elle serait en bonne partie difficilement exploitable. C'est le croisement des données qui devient fécond. De sorte que le stockage ne peut certainement pas consister simplement en une sorte d'entassement ou d'alignement, mais se présente lui-même comme une sorte de construction architectonique et cohérente.

---

[374] James STATEN, How to turn cloud economics to your advantage *: https://azure.microsoft.com/nl-nl/blog/how-to-turn-cloud-economics-to-your-advantage/*

b. <u>Le stockage intelligent et indiscret</u>

466. Jadis déjà, dans les années qui précèdent, les entreprises mettaient déjà en forme leurs données grâce aux techniques dites de la « *Business Intelligence* ». Toutefois, cette façon de faire - bien classique, se présente dorénavant comme trop limitée et dépassée. Ainsi, de nouveaux outils, dotés d'une forte capacité d'analyse, ne vont pas tarder à révolutionner le stockage et l'utilisation des données.

Le *big data* n'est donc pas seulement un fait déjà établi et dont on peut faire le tour, mais, avant tout - sans doute - un domaine potentiellement considérable, non encore exploré ; et certainement non encore explorable. Il semble vertigineux. Par conséquent, l'exécutif ou le législateur se sentent quelque peu débordés.

467. De nouveaux défis sont à relever ; de nouvelles exigences s'imposent. L'amélioration de la performance industrielle, le développement commercial et une meilleure connaissance des clients. Depuis un certain temps déjà, le *data mining* permettait de mettre en relation différentes données. Il constitue une composante essentielle des technologies que l'on peut traduire comme faisant de " l'exploration de données ", parfois même de " la classification de données ". Même si cette dernière notion est trop statique.

En réalité, il s'agit plutôt d'un processus dynamique d'investigation. On osera parler d'une sorte " d'alchimie de données brutes ", transformées en informations utiles, pour l'organisation des services publics, mais aussi et surtout par des entreprises. Dans le dessein évident d'augmenter leur chiffre d'affaires et de mettre en œuvre une nouvelle approche marketing.

En définitive, de nouveaux logiciels *data mining* constituent des outils de plus en plus indispensables, dans le but de relier différentes bases de données. Ils sont formés d'algorithmes très sophistiqués, qui demandent des ordinateurs puissants, afin de pouvoir traiter une abondance de données. Les innovations constantes favorisent leur fonctionnement. Il reste à se demander comment le droit peut affronter ce nouveau phénomène.

Par ailleurs, dans la même ligne de progrès technologique, nous pouvons citer la *Data Warehouse*. Il s'agit d'un procédé permettant de centraliser la gestion et la recherche des données, complétant ainsi les atouts du data *mining*.

Ainsi, les entreprises sont-elles en mesure de diviser les données en segments d'utilisateurs précis. Ce qui en permet une meilleure analyse, et surtout une meilleure utilisation. En termes

plus simples, on pourrait parler d'un " répertoire central ", ou " centralisé ". Les avancées technologiques ont permis de réaliser ce qui semblait relever du rêve.

468. Le *data mining*, un processus dynamique (non pas une sorte d'accumulation inerte) peut ainsi passer par différentes fonctionnalités de plus en plus évoluées : l'association, l'analyse de séquences, la classification, le clustering (l'identification visuelle de groupes de faits inconnus), et surtout la prédiction qui est l'opération la plus recherchée. Le *data mining* est salué comme une bénédiction non seulement dans les mondes de la finance et de l'entreprise, mais également dans celui de la recherche. Du point de vue intellectuel, il se présente comme redoutablement stimulant. Ceci, dans la mesure où il met en évidence le lien entre l'interne et l'externe, par exemple le prix et les modes de consommation.

    Au travers de la détermination et de l'articulation concrète d'un grand nombre de données, il est possible d'évaluer : les succès à venir, le nombre des ventes, notamment. Il permet l'envoi des promotions ciblées, soigneusement choisies en fonction du profil des destinataires, à des moments de l'année précis.

469. Le *data mining* permet également de repérer une tendance associée à une autre. Par exemple, si tel jour, tel produit est acheté de façon plus abondante que tel autre, il est possible qu'un tel produit soit également davantage recherché tel même jour. Par exemple, le samedi, les gens achètent davantage de quoi faire un sandwich pour le lendemain (le dimanche), mais également des cannettes de bière ; non seulement en vue du dimanche, mais parce que l'achat d'un sandwich (à savoir de quoi manger sur le pouce) les incite un peu automatiquement à ajouter de quoi boire, sur le pouce.

470. Ce constat est évidemment fort utile pour le commerce et le commerçant, à toute échelle. Il incite à vendre des bières non loin du pain pour les sandwichs. Cet exemple est évidemment très simple, mais il va de soi que les applications sont souvent beaucoup plus conséquentes. L'action prédictive permet également d'anticiper le manque d'un produit à certains moments et de pallier certaines fluctuations. L'analyse des signaux d'une chaîne de production incite également à des réparations et à des changements avant que les pannes ne se déclarent. La détection des fraudes en amont s'avère particulièrement indispensable parfois.

471. Quant à l'analyse des comportements passés et présents des clients, également dans la perspective de prédictions futures (qui sont souvent présentées comme aléatoires et relevant du hasard, mais sans doute à tort), elle devance les difficultés et maximise les opportunités.

Tout l'intérêt de ces techniques est d'envisager des hypothèses prédictives sur des événements à venir, particulièrement intéressantes dans le domaine du marketing.

472. L'analyse prédictive se fonde sur une capacité à mettre en relation de nombreux facteurs impliqués, qui rendent effectivement complexes la détermination du futur, mais donnent un aperçu du possible. Une telle technique paraît singulièrement opportune pour évaluer le risque-client en matière financière, par exemple quant aux chances de remboursement effectif d'un crédit. Un ensemble de données sont prises là en compte, par exemple les antécédents du client, ses remboursements ou non de par le passé, les découverts et les retards, mais également : la catégorie socio-professionnelle qui est la sienne, le contexte économique dans son ensemble, et de nombreuses autres variantes.

Plus les données sont nombreuses et précises, judicieusement croisées, plus l'analyse statistique a des chances d'être juste. L'analyse prédictive associe des variables explicatives et des variables expliquées, ou prédites, pour évaluer une probabilité plus ou moins forte qu'advienne telle occurrence. Nous sommes - bien entendu - dans de l'hypothétique. D'autres imprévus sont - hélas ou heureusement d'ailleurs - toujours possibles. Selon une phrase célèbre, « le battement de l'aile d'un papillon peut provoquer un ouragan ». C'est justement ce que l'on appelle quelquefois « l'effet papillon ».

Parfois résumé de façon simplifié en disant que de petites causes lointaines découlent de grandes conséquences futures. En 1972, lors d'une conférence scientifique demeurée célèbre[375], le scientifique américain Edward Lorenz (1917-2018) posait cette question : « Le battement d'ailes d'un papillon au Brésil peut-il provoquer une tornade au Texas ? » Il faisait allusion à une interrogation ironique du philosophe français Denis Diderot se demandant si la ruade d'un cheval dans la campagne française pouvait perturber le vol d'un papillon sur une île lointaine. Lorenz développe de façon très claire son point de vue : la modification d'une donnée initiale peut avoir de lourdes conséquences à l'arrivée.

473. L'analyse prédictive se montre donc très sensible à la moindre évolution des données de départ. Celle-ci peut agir dans un sens positif, comme dans un sens négatif, de même qu'un seul battement d'aile d'un papillon peut certes susciter une tornade mais également l'empêcher. La difficulté que surmonte - en partie - l'analyse prédictive est que des causes semblables (et à

[375] Traduction française : Edward N. LORENZ, « Un battement d'aile de papillon au Brésil peut-il déclencher une tornade au Texas ? »,in *Alliage*, 22, 1995, 42-45

peine différentes) peuvent bien susciter des effets en revanche dissemblables et fortement différents. Ce qui exige une précision et frappe de précarité toute approche imprécise.

Là où l'analyse prédictive revêt une importance extrême, c'est bien entendu dans la climatologie. Une petite donnée modifiée peut introduire un important changement climatique. Les mathématiciens ont donné toute son ampleur à ce que l'on appelle " la théorie du chaos "[376]. Les questions techniques qui se posent sont éminemment difficiles. Cependant, elle donne une autre image du déterminisme - qui existe peut-être toujours, mais ne se dégage plus avec la même netteté. De même que l'on évalue avec des probabilités statistiques le risque qu'il se mette à pleuvoir dans quelques heures. Chaque position initiale de l'atmosphère a certainement un futur unique, dont la solution existe, mais ne peut pas en trouver l'équation : on ne peut pas écrire la formule qui donnerait la solution, on peut tout au plus dégager une probabilité. En matière de prévisions météorologiques à court terme l'intervention du facteur humain (et tout ce qui relève de la sphère privée de l'individu) n'interfère en aucune manière.

Il en va bien différemment des prévisions liées aux décisions et aux intentions des individus. La théorie du chaos contraint, d'une certaine façon, les analystes à une investigation singulièrement poussée ; rendue permise par les *big data* et par une accessibilité extrême des données.

474. Le droit se doit donc de tenir compte d'une telle utilité et d'une si forte motivation. Les modèles prédictifs analysent les performances passées pour estimer la probabilité que peut avoir un client de montrer un comportement spécifique dans le futur ; dans la perspective d'améliorer la performance à venir.

Les modèles prédictifs effectuent souvent des calculs durant les transactions en ligne, dans le souci de limiter les risques. On peut craindre une double intrusion dans la vie privée des individus : d'une part, de façon directe, dans la quête des informations. D'autre part, de façon indirecte, par la simulation des ordinateurs qui d'une certaine manière peuvent prévoir de façon encore plus rapide et précise ce que quelqu'un fera ; que ce quelqu'un ne pourrait faire. Ce qui, d'une certaine manière, donne le tournis.

475. Les modèles descriptifs quantifient les relations entre les données, souvent de façon à classer les clients ou les prospects dans des groupes. Ce qui peut sembler discriminatoire et réducteur. En effet, de plus en plus, il ne s'agit pas seulement de s'intéresser à un seul comportement de

[376] Ivar EKELAND*, Le chao*s, Paris, Flammarion, Dominos, 1995 ; James GLEICK, *La théorie dui chaos*, Paris, Albin Michel, 1989 ; David RUELLE*, Hasard et chaos,* Paris, Odle Jacob, 1991.

client, mais à faire différentes prévisions, envisageant diverses hypothèses de relations entre les clients ou entre produits. Dans le but d'imaginer de meilleures solutions, toujours pour une plus grande rentabilité.

À l'arrivée, il s'agit bel et bien de modèles de décisions utilisés pour développer une logique cohérente. Afin que l'action souhaitée se produise, pour chaque client, ou dans chaque circonstance. On peut penser que ce but visé relève de l'asymptote, dont on se rapproche de plus en plus sans jamais l'atteindre. Toutefois, cette limite ne décourage pas du tout l'analyse prédictive, au contraire. Du reste, un risque statistique non nul, mais extrêmement bas, peut-être considéré comme insignifiant. Donc, l'analyse prédictive peut bel et bien être utilisée dans un grand nombre d'applications ; revêtir un impact véritablement important. C'est, par exemple, le cas dans le domaine de la santé : pour évaluer les risques que courent tels ou tels patients de développer des maladies comme le diabète, des troubles cardiaques, ou tel ou tel cancer. L'analyse prédictive permet, ainsi, de mieux orienter le choix des médecins et des patients.

Elle se montre également fort utile en matière de recouvrement financier, par exemple. Elle permet de mieux identifier les agences les plus efficaces ; les stratégies de contact et les actions judiciaires éventuellement à mener, toujours au cas par cas.

476. Comme on peut le deviner, une telle analyse est, par ailleurs, particulièrement utile aux fournisseurs d'assurances. Qu'il s'agisse d'une assurance automobile ou d'une assurance santé. Dans ce dernier cas, l'analyse prédictive peut aider à analyser les données du passé médical et à évaluer le coût que l'assuré pourra faire peser sur elle. Toujours est-il qu'une analyse prédictive bien menée peut en effet réduire des risques de défauts de paiement et contribuer à mieux déterminer les taxes à acquitter dès le départ. Cependant, on perçoit d'emblée les risques importants ; par exemple dans le domaine de la santé, de porter atteinte au droit du patient à la confidentialité. En effet, les assurances voudront connaître au mieux tous les facteurs de risque concernant les patients. Une seule donnée oubliée fausse totalement la prévision.

477. C'est là que l'attention du juriste doit absolument - et de toute urgence - être portée. En effet, l'utilité évidente de l'analyse prédictive ne justifie pas toutes les possibilités d'y avoir recours. Il faut songer à des garde-fou, en amont et aval. Ce qui protège le secret et assure l'oubli possible.

Section II : Du secret et de l'oubli.

478. Ainsi, chaque citoyen dispose d'un véritable droit à la protection de sa vie privée : qu'il s'agisse de la divulgation d'informations, ou de leur diffusion diffamatoire ; mais également du fait de divulguer ce qui ne doit pas l'être.

On le sait, le droit à la protection de la vie privée a été affirmé en 1948 par la Déclaration universelle des droits de l'homme des Nations unies (art. 12). En droit français, l'article 9 du Code civil, introduit par la loi du 17 juillet 1970, dispose que : « Toute personne a droit au respect de sa vie privée ». Cette protection a été spécifiée et étendue par diverses décisions du Conseil Constitutionnel.

479. Un grand principe passe bien entendu par des protections très concrètes. Ainsi, de nombreux pans de l'existence sont concernés par l'essor des big data. Ce qui peut avoir des impacts négatifs. Nous en dresserons plus loin l'inventaire.

a. La vie privée

480. Tout ce qui est du domaine privé, se distingue de ce qui est du domaine public. Le mariage, par exemple, n'est évidemment pas dans le domaine privé. Ce n'est pas porter atteinte à la vie privée que de révéler qu'une personne est mariée ; sauf contexte tout particulier par exemple de persécution ou de dictature.

481. Cette mise au point, nous allons le voir, ne résout pas toutes les difficultés. Elle montre que le problème est - sans aucun doute - plus complexe. Le statut matrimonial peut certes constituer en soi des données qui relèvent de ce qui est public, de ce que tout le monde a le droit de savoir, mais peuvent pourtant créer des discriminations.

En effet, indiquer l'âge sur son *curriculum-vitae* lorsqu'on cherche un emploi peut nuire à la personne car l'employeur potentiel écartera une personne qui lui semble trop âgée ou en revanche une autre qui est mariée et a des enfants, car ayant moins de temps à consacrer à son travail, étant moins disponible et surtout moins mobile On le voit, la question de la protection de la personne - au travers de la protection de sa vie privée, s'avère beaucoup plus complexe que de tracer une ligne de partage entre tel type d'information et tel autre. Il présente un risque de discrimination.

482. Au fil des âges, en Occident, vont émerger des valeurs individualistes renforçant - par corollaire - l'idée d'une sphère privée. Concrètement, la fin de la promiscuité, ainsi qu'une meilleure qualité de vie – mais par pour tous de façon égale – vont contribuer à une volonté de tranquillité, qui va se caractériser par des normes législatives protectrices.

En réalité, l'évolution historique peut sembler paradoxale. D'une part, elle se caractérise par un souci de ne pas être livré au regard indiscret et curieux de l'entourage proche, par exemple du voisin. D'autre part, l'essor de la presse, puis de la photographie, puis du cinématographe, vont - d'une certaine façon - ouvrir la voie à des formes d'indiscrétion beaucoup plus inquiétantes, et à une échelle beaucoup plus large surtout.

483. Ce paradoxe doit constamment être gardé à l'esprit. D'une part, l'indiscrétion du proche devient insupportable. Il est vrai aussi qu'elle peut compromettre une vie commune ou une collaboration, ou encore faire peser une pression psychologique insupportable et constante. De l'autre, l'indiscrétion d'inconnus, ou d'un vaste public, peut être entretenue. On peut se demander s'il s'agit bien du même type d'indiscrétion, d'une indiscrétion de la même nature. En effet, les deux types peuvent sans doute se croiser.

484. Ainsi, le voisin de palier peut bien entendu découvrir les secrets cachés de sa voisine par voie de presse. Mais, de façon abstraite. On peut néanmoins considérer qu'il s'agit de deux genres d'indiscrétions de nature bien différente. Ce sont deux avocats de Boston, Samuel Warren et Louis Brandeis qui donnent, en 1890, toute sa résonance à l'idée de défense de la vie privée, associée à la protection de la tranquillité, au droit à être tranquille : *« the right to be let alone »*[377]. Le souci des deux avocats est bien de combattre les abus de portraitistes, et aussi l'exploitation commerciale qui peut être faite des portraits. En même temps, ces deux avocats sont conscients qu'une page nouvelle est en train de s'ouvrir ; que l'essor des techniques va créer une situation inédite et un monde nouveau, ceux que le droit aujourd'hui tente de réguler.

b. <u>Un discernement complexe et discutable</u>

485. La Convention européenne des droits de l'homme, dans ses principes directeurs, rappelle le caractère objectif des droits de l'homme. Elle prend appui sur ceux-ci, les reprend et répète. Il ne s'agit pas de droits attribués aux individus par le biais d'un statut juridique particulier,

[377] Louis BRANDEIS et Samuel WARREN, « The right to be let alone », in *Harvard Law Review*, 1890-1891, 192-223. Cf. aussi Philippa STRUM, *Beyond Progressivism*, Kansas, University Press of Kansas, 1993.

potentiellement révocable, mais de droits qui sont attachés à la seule qualité de personne humaine. Sous toutes les latitudes et dans tous les contextes

Les droits concernés sont énoncés par la Convention dans son titre I et ses Protocoles 1, 4, 6 et 7. Il s'agit avant tout de droits individuels : c'est-à-dire de droits dont l'individu est titulaire. Ils visent à protéger la liberté et la dignité de l'homme : ce sont des droits civils et politiques.

Les droits économiques et sociaux sont eux énoncés, ailleurs, dans la Charte sociale européenne de Turin de 1961. Ils n'obéissent pas à une parfaite symétrie avec les droits de l'homme *stricto sensu.* La Convention européenne des droits de l'homme a été rédigée avant la déferlante numérique. Paradoxalement le risque, pour la démocratie, est aussi lié à la volonté de promouvoir la démocratie. En effet, la dissimulation des données, surtout lorsque cela touche - d'une certaine façon - la collectivité (par exemple, au travers de la figure d'un responsable public), est perçue de façon tout aussi négative que la violation de la vie privée.

486. On ne se trouve pas tant, en cette matière, face à une menace clairement définie (à conjurer), mais plutôt face à deux menaces conjointes. À deux exigences, aspirations et tension. Ce qui rend la tâche du législateur et du juge plus ardue. Beaucoup de problèmes concrets se posent, dont la résolution devient urgente dans le contexte actuel d'explosion de la révolution numérique (mais qui - en définitive - existaient avant et sont indépendants).

L'un d'entre eux est de savoir ce qui relève - ou non - de la vie privée : de sa mesure, de ses limites. Cela vaut, par exemple, pour la religion ; que l'on ne peut sans doute totalement identifier à la seule conviction personnelle en matière religieuse, appartenant à la seule sphère intime. La foi privée (ou son absence) est une chose. L'appartenance à un groupe bien défini se déployant forcément dans la sphère publique se présente comme plus complexe.

487. L'évaluation de ce qui est privé et de ce qui est public peut varier au fil du temps. Comme, d'ailleurs, la conception-même de ce qu'est la laïcité qui n'a pas toujours été identique, et de loin.

Ainsi, le 10 mai 1912, en France, le Conseil d'Etat refusa à un prêtre de s'inscrire sur les listes du concours à l'agrégation de philosophie, en raison de son statut personnel[378]. À l'évidence sa condition sacerdotale n'était pas considérée comme relevant de la sphère privée, mais plutôt comme susceptible de porter atteinte à la laïcité.

[378] Maurice HAURIOU, */www.revuegeneraledudroit.eu/blog/2013/11/27/refus-du-ministre-dadmettre-un-pretre-catholique-sur-la-liste-des-candidats-a-un-concours-dagregation-de-lenseignement-secondaire/*

488. En 1972, sur la même question de l'acceptation - ou non - d'un prêtre dans l'enseignement secondaire, le même Conseil d'Etat a porté un jugement exactement inverse de celui de 1912. Pour lui, en effet, dans un décret du 21 septembre 1972, il n'était pas fondé d'établir une discrimination à l'embauche dans l'enseignement secondaire en raison de l'état ecclésiastique. Cet état étant une données personnelle,[379]. Ainsi, la neutralité du fonctionnaire ne concerne pas son histoire ou son statut personnel, mais son attitude.

En 2018, le Conseil d'Etat a précisé qu'un prêtre – toujours en exercice (le cas des « défroqués » est autre, car ils ne sont plus considérés socialement comme prêtre) - peut devenir Président d'une Université. Ce qui relève de l'enseignement supérieur n'est sans doute pas applicable au secondaire ; ou, avec d'autres critères[380]. Cette décision a été rendue sur une affaire s'étant déroulée en Alsace, terre concordataire, où la laïcité peut avoir un sens plus élastique. Il semble - tout de même - que l'avis en question vaut pour toute la France.

489. On peut également se demander si l'appartenance religieuse relève - ou non - de la vie privée. Le Code pénal réprimant toute discrimination en fonction de celle-ci. Cela suppose qu'elle puisse être invoquée en dehors de la vie privée bien qu'elle ne relève pas, en France, de l'état civil. Une appartenance publique ouverte, par exemple à cause du costume porté ou de propos tenus n'exclut pas dans d'autres cas que l'on puisse considérer la religion comme relevant d'une sphère plus discrète ? En effet, les lignes de frontières ne semblent pas toujours faciles à tracer, entre ce qui relève du privé et du public. On peut quelquefois se demander si la ligne de partage (loin de suivre - au fond - des distinctions entre disciplines) ne tient pas plutôt au risque éventuel de nuisance d'une information connue et d'une révélation faite.

490. Le discernement devrait donc être élaboré, en aval, et non en amont. Ainsi, la foi religieuse, ou l'orientation sexuelle, ne relèveraient pas exclusivement de la sphère privée, en soi, mais seulement dans certains cas ; en raison des risques encourus par la personne en cas de dévoilement.

À l'inverse lorsqu'une personne fait du prosélytisme par exemple homosexuel religieux, il est évident que cela ne relève plus de la sphère privée. Cela relève du fait même de la conduite de l'intéressé, qui n'a qu'à s'en prendre à lui-même : s'il estime que tel aspect de sa personnalité est désormais notoire.

---

[379] *http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Dossiers-thematiques/Le-juge-administratif-et-l-expression-des-convictions-religieuses*

[380] *www.la-croix.com/Religion/Laicite/Le-Conseil-dEtat-confirme-quun-pretre-peut-presider-universite-2018-06-b.29-1200951215*

491. L'enjeu, du point de vue juridique, est que les distinctions ne soient pas forcément faciles à établir et que les frontières soient mouvantes et poreuses selon le contexte. Une possible conception de la sphère privée, comme recouvrant ce qui ne saurait être dévoilé - au moins sans risque pour la personne concernée - est évidente. Ce qui est notoire - ou manifesté de façon claire par la personne elle-même, même à ses dépens, n'entre pas ici en ligne de compte.

Cela peut paraître problématique. Dans une certaine mesure, on peut même se demander si toute révélation ne risque pas, plus ou moins directement, d'attirer des dommages et des ennuis, du reste, vraiment mineurs quelquefois, à la personne concernée.

492. " Y-a-t-il réellement des données concernant une personne totalement neutres, c'est-à-dire ne suscitant pas de l'hostilité ou au moins de l'agacement ? Faut-il alors affiner encore le critère en tenant compte d'un certain ordre de probabilité ? Faut-il alors considérer qu'il y aurait violation éventuelle de la sphère privée lorsque telle donnée expose telle personne à un risque suffisamment consistant avec tel pourcentage de probabilité ? Mais qui déterminerait et en fonction de quelles mesures se voulant objectives un tel pourcentage de probabilité ?"

Autant de questionnements possibles. Pourtant, cette nouvelle conception peut également être conçue comme singulièrement pertinente. En effet, ce qui gêne quelqu'un, concrètement, dans l'atteinte à la vie privée, ce sont les inconvénients pour lui d'une révélation. Même si ces inconvénients ne sont pas vraiment contestables (comme, par exemple, une peine judiciaire, ou une attaque physique, ou la perte d'un emploi). Cependant, ils entraînent la perte de l'estime attendue d'une ou de plusieurs personnes.

493. Il est vrai que, très souvent, nous l'avons dit (et ce pourtant des motifs variés) les personnes se mettent quelquefois elles-mêmes dans la situation de s'attirer des ennuis ; faute d'avoir réfléchi, d'avoir évalué l'impact d'un post sur *facebook* par exemple. Toutefois, quand bien même quelqu'un est l'artisan de son propre malheur, ce n'est évidemment pas une raison d'en rajouter et d'en créer un nouveau, même peu probable ou moins ravageur.

Les hommes politiques redoutent la diffusion de toute révélation pouvant porter atteinte à leur carrière, pouvant dissuader des électeurs de voter pour eux. Un artiste ne doit pas décevoir tous ceux qui placent en lui leur confiance. La révélation de certains secrets peut faire perdre sa popularité à un acteur. Par exemple, l'homosexualité d'un acteur américain, peut décevoir ses fans féminins qui n'iront plus voir ses films.

494. Dans la mentalité contemporaine, au moins dans les pays d'Europe occidentale et aux Etats Unis, la question s'envenime. Ceci, dans la mesure où l'idéal de transparence et d'authenticité s'impose de façon plus forte que jamais. Un politicien fustigeant certaines pratiques, par exemple sexuelles, qui sont pourtant les siennes, a-t-il encore le droit de protéger certains pans de son existence du regard indiscret, et parfois vengeur, de la presse et de l'opinion ? Spontanément, il serait tentant de répondre de façon positive. En effet, le droit en question a une valeur et une légitimité en lui-même ; peu importe le contexte et le fait que l'intéressé vive - par ailleurs - dans le mensonge : qu'il trompe ses électeurs sur sa personnalité réelle. Sans aucun doute, le problème semble plus complexe. Le droit de protéger sa vie privée n'est pas absolu. Il suppose certaines conditions.

495. Certes, en règle générale, il s'impose et doit être défendu, mais on peut néanmoins estimer qu'il existe des exceptions. Un *serial killer*, cachant soigneusement ses viols, ne peut certainement pas arguer d'un tel droit pour contester la révélation de ses forfaits. Dans le cas d'un politicien en campagne, par exemple, on peut considérer qu'il choisit lui-même de descendre dans l'arène et de se soumettre au jugement de l'agora. Qui plus est, il donne une image de lui-même et souvent la complète et l'explicite par des convictions affichées et des affirmations proférées (par exemple lorsqu'il prétend être d'une totale intégrité morale, sexuelle ou financière) Cela se corse encore s'il s'en prend à la moralité des autres, alors qu'il fait la même chose ou pire encore (comme, par exemple, tromper le fisc).

496. Un mensonge public ne peut-il pas être mis en cause, à partir d'éléments qui relèvent certes en temps normal de la sphère privée, mais qui d'une certaine manière ne sont pas si privés que cela. Ou, du moins, ne le sont plus totalement, dans la mesure où l'intéressé est sorti du cadre de la vie privée. Il entend mener une vie publique, et, surtout, semble fonder sa propre légitimité sur une rigueur morale dont il est en fait dépourvu. Dans la mesure où ses déclarations publiques ne correspondent pas à la réalité cachée, il n'y a plus seulement une confidentialité sauvegardée, mais encore une vraie tromperie. Cette dernière est fondée à partir de fausses déclarations ou de prises de position ne correspondant pas à ce qui est vécu, voire se situant en totale opposition.

497. On songe, dans « les Aventures de Tintin » d'Hergé, au Capitaine Haddock, buveur invétéré de whisky, qui préside en même temps … la ligue antialcoolique. Familièrement, on dirait : « Faites ce que je dis, et non ce que je fais !» Pendant longtemps, l'opinion dominante dans le monde occidental était qu'il s'agissait, en définitive, d'un dernier – ou premier – hommage que le vice rendait à la vertu. À défaut de pouvoir vivre selon les normes éthiques que l'on affiche, au moins on les défend, et on les promeut. Le pire, au fond, serait de vouloir justifier le mal que

l'on fait (voire même que l'on a déjà fait), de l'afficher. Ce qui crée ainsi un scandale. Sur ce point, la mentalité a considérablement évolué, probablement en grande partie à cause d'une prédominance croissante de la façon de voir des Anglo-Saxons sur celle des Latins.

498. Les révélations en cascades concernant les abus sexuels, dans différentes sphères de la société, constituent certainement, à cet égard, la confirmation la plus manifeste d'une évolution de la société mais également ce qui va encore s'accroître. L'*omerta* maintenue, la dissimulation pour sauver la façade (ou le prestige d'une institution) sont considérées comme des fautes très graves.

De même, un discours moralisateur tenu par une personne qui ne vit pas ce qu'elle dit, même si théoriquement elle voudrait peut-être le vivre, n'est plus du tout considéré comme une manière de servir le bien par le verbe à défaut de le faire par les actes mais plutôt comme une tromperie, comme si l'on aggravait encore la faute d'une mauvaise conduite par le mensonge à son sujet. Très significative en son temps, d'une mentalité plus anglo-saxonne, mais qui est plus largement ouverte (peut-être comme un fruit empoisonné ou un dommage collatéral de la mondialisation a été l'affaire Clinton) que celle d'un passé relativement récent.

499. Comme chacun le sait, le président américain d'alors, Bill Clinton se trouvait au cœur d'une tornade médiatique particulièrement déchaînée ; qui aurait pu lui coûter sa présidence. À cette époque, cet épisode fut surtout évoqué dans le monde occidental pour se moquer du puritanisme des Etats-Unis. En réalité, on aurait été mieux avisé d'y voir une certaine cohérence intellectuelle et morale, en bonne part étrangère ; par rapport à une sensibilité plus latine il est vrai, mais qui risque de se diffuser et d'être confortée par le développement technologique et la multiplication vertigineuse des données..

500. Bill Clinton - on s'en souvient - avait menti, sous serment qui plus est, en niant avoir eu des rapports sexuels avec Monica Lewinsky. Avant de finalement le reconnaître, plus ou moins face à l'évidence. Là encore, ce n'est pas tant l'adultère qui est en cause, mais le mensonge. Le plus grave, aux yeux des Etats Unis, n'était certes pas, de la part de Clinton, d'avoir eu cette relation hors mariage, mais d'avoir ajouté, à cette faute de faiblesse, en dernière instance assez compréhensible et excusable, une faute bien moins vénielle de mensonge sinon de parjure.

C'est dans le contexte de cette nouvelle mentalité que le droit doit se définir, pour l'intégrer, mais aussi, peut-être, pour la limiter, pour en freiner les excès et en tempérer l'intransigeance vengeresse.

501. En Europe occidentale, l'homosexualité est largement admise, et même reconnue souvent et institutionalisée, par exemple avec le « mariage pour tous » en France.

502. En revanche, malheur à celui qui exprimerait un jugement critique sur des mœurs homosexuels. surtout dans le cas où il en aurait lui-même en cachette. Ce point montre, au moins dans une partie dominante de la population, un retournement complet de l'opinion. Même s'il n'est certainement pas non plus unanime, et de loin.

On peut, par exemple, penser aux manifestations hostiles à ce même « mariage pour tous ». Il n'empêche. L'opinion tolère de moins en moins une contradiction entre la sphère privée et ce que l'on montre dans la vie publique. Il y a encore cinquante ans, avoir une maîtresse cachée et faire par ailleurs l'éloge de la fidélité conjugale n'était pas forcément considéré avec sévérité, mais plutôt avec une certaine indulgence. Aujourd'hui, un tel clivage entre l'apparence et la réalité est dénoncé avec une grande sévérité.

503. Il ne s'agit pas simplement d'une maladresse ou d'un zèle inapproprié, mais d'une déloyauté et d'un mensonge. L'authenticité - par rapport à soi-même - est considéré comme une valeur première. De tout temps, une faute avouée pouvait être à moitié pardonnée, comme on le dit souvent, mais désormais, nul n'est habilité à prononcer un jugement moral, et a fortiori à critiquer une conduite, s'il ne donne pas lui-même un exemple sans faille.

504. Or, la multiplication des données qui circulent rend délicate une double vie, cloisonnée, avec deux cohérences, en contraste, pour ne pas dire plus. L'affaire Jérôme Cahuzac doit également être située dans ce contexte. Au fond, ce ne sont pas tellement les malversations financières de l'homme qui choquent, mais plutôt le fait qu'il ait été ministre délégué au Budget ; pourfendeur de la corruption et de la fraude fiscale ! « Faites ce que je dis et non pas ce que je fais ».

505. Les nouvelles technologiques rendent plus difficile cette attitude ambivalente, qui fut par exemple celle d'un Colbert sous Louis XIV. L'opacité protectrice n'est plus acceptée, et devient toujours plus difficile. Du point de vue philosophique, comme du point de vue juridique, l'évaluation de cette évolution doit être nuancée.

D'une certaine manière, comment nier un certain progrès moral dans le fait de vouloir rompre avec une culture de la corruption et du mensonge ? Mais ne court-on pas un risque inverse ? Faut-il toujours dire la vérité ? Ou, y-a-t-il des cas où la prudence et la sagesse en dissuadent ? On connaît le débat philosophique sur la question entre Kant et Benjamin Constant[381]. La question n'est pas facile à traiter. Certes, dans des cas extrêmes, par exemple si la Gestapo

[381] Johann RIVALLAND, Le droit de mentir de Benjamin Constant : h*ttps://www.contrepoints.org/2017/10/25/132377-le-droit-de-mentir-de-benjamin-constant*

demande à quelqu'un s'il cache un juif (ou un résistant chez lui) personne – on ose l'espérer – ne soutiendra qu'il faut dire la vérité.

506. À l'évidence, il y a des exceptions à la règle. Habilement, certains théoriciens parlent de la légitimité de la restriction mentale. Lorsqu'un importun sonne à la porte, la bonne répond : « Monsieur n'est pas là ». Voulant dire en fait – mais sans le dire – « Monsieur n'est pas là pour vous ».

On peut cependant y voir une dérobade, et une justification assez « tirée par les cheveux ». En amont, ne faudrait-il pas plutôt considérer que l'obligation de dire la vérité n'est pas absolue et constante, mais suppose certaines conditions ?

507. Nous voici à nouveau plongés dans une nouvelle perplexité, celle du cas par cas ; au-delà d'une solution abrupte et toute faite. La prise de conscience doit y jouer un grand rôle. Le droit semble donc devoir respecter cette complexité ; et susciter cette délibération sans ne la court-circuiter ni simplifier des enjeux parfois multiples. Un nouveau rôle, donc, pour le juriste, à la fois plus modeste, et plus ambitieux.

Or, le développement des médias, et l'évolution des mentalités, induit l'idée selon laquelle le public aurait plus ou moins le droit de tout connaître des hommes d'Etat, des candidats à une élection ; voire, plus largement, d'un acteur qu'il admire. Toute discrétion serait presque un mensonge par omission. Le *paparazzi*, à savoir le photographe indiscret (comme celui que l'on retrouve dans le film célèbre de Federico Fellini « *la dolce vita* »), ferait presque figure de reporter héroïque ; qui a le droit de découvrir ce qui est caché et de le faire connaître à tous.

508. À l'évidence, cette nouvelle mentalité situe autrement le débat juridique ; sur les peines à appliquer - ou non - dans le cas de photos volées et diffusées, notamment. Notre époque serait donc celle de la disparition de la vie privée ; sinon pour ceux dont les secrets ne suscitent aucun intérêt pour personne. Et encore, car le pittoresque de certains épisodes vécus par eux pourrait au contraire alimenter des curiosités. Dans certaines de nos émissions télévisées, c'est « Monsieur Tout le monde » qui parle de sa vie personnelle, avoue ses problèmes et confesse ses turpitudes. Faut-il donc comme Jeff Jarvis en 2011[382] dire que la vie privée n'existe plus, même si une telle affirmation sonne de façon tout-de-même péremptoire ? Quelles implications, le juriste doit-il - ou peut-il - en tirer ? Doit-il s'opposer et résister ? Faut-il qu'il se résigne à l'inéluctabilité d'une situation encore vouée à se renforcer ?

[382] *http://www.slate.fr/story/33281/jeff-jarvis-google-allemagne*

509. L'une des réponses quelquefois apportées est que personne n'est obligé, malgré l'effet de mode et le panurgisme contemporain, de se confier sur les réseaux sociaux. Aucune loi n'oblige qui que ce soit à utiliser l'Internet. En théorie. En effet, dans la pratique, être totalement déconnecté implique une mort sociale. Certes, il est vrai que le dévoilement de sa vie privée - ou au moins de certains éléments la constituant - est souhaité par nombre d'entre nous. Il n'en demeure pas moins que le risque d'atteinte à la vie privée est considérablement augmenté, par les technologies de l'information. Plus une personne se livre sur l'Internet, plus sa vie privée risque d'être réduite à néant ; justement en raison du croisement des données, dont nous avons parlé plus haut.

510. L'addition des données correspond - de fait - à la multiplication de ce que l'on peut savoir et déduire. Sans doute, dans une grande majorité de cas et de situations, il n'y a pas à redouter véritablement - dans l'immédiat - une utilisation vraiment totalitaire des données.

Dans la société française, personne n'est inquiété pour ses opinions ou sa façon de vivre, si elle est conforme à la loi.

Nonobstant, le risque d'une dérive totalitaire est toujours possible. De voir émerger un nouveau Staline et un nouvel Hitler. Peut-on vraiment exclure une forme de contrôle totalitaire moi d'un système plus que d'une personne ou d'un groupe ?

Au moins à titre purement hypothétique, il est avisé d'imaginer l'usage qui pourrait être fait des données laissées sur l'Internet, qui seraient recoupées. De plus, même si nous vivons une époque de plus grande tolérance dans le monde, ce n'est pas le cas partout ; et de loin, sur la planète.

511. Enfin, des inconvénients moins dramatiques et scandaleux existent pourtant d'ores et déjà. Une telle confiance en l'Internet peut ainsi donner une mauvaise image d'une personne. Ce qui pourrait compromettre son embauche. La liste des livres achetés ou empruntés pourrait indisposer un ami ou un proche qui ne partagent pas vos goûts ou vos convictions.

512. Au début des années 2000, Simson Garfinkel[383], dans un livre très intéressant (et au demeurant fort suggestif), sur la fin programmée et rapide de toute *privacy*, dénonce l'intrusion croissante - phagocytant - de l'Internet : les précautions d'anonymisation prises étant inefficaces, et

[383] Simson GARFINKEL, *Database Nation; The Death of Privacy in the 21st Century*, New York, 2000, O'Reilly and Associates.

adroitement contournées. Certes, il y a bien des chances et des promesses dans la *publicness* dont parle Jarvis. En effet, d'une certaine façon, s'il est intelligent et habile, l'internaute parvient bien à façonner lui-même l'image qu'il entend donner à l'Internet. On peut donc envisager un effet paradoxal : d'une part l'Internet, peut nous trahir, mais nous pouvons aussi nous servir de ce média pour composer une nouvelle image de nous-mêmes. Comme certains auteurs qui écrivent leur propre biographie, non pas tellement pour se dévoiler, mais pour dissimuler ainsi habilement certains pans de leur existence.

513. Il faut, dans le contexte actuel, mesurer non seulement le risque intrinsèque que fait peser notre action, mais aussi les risques beaucoup plus conséquents liés au piratage. Des données confiées dans l'idée qu'elles seraient en sécurité peuvent, hélas, facilement être piratées. Indépendamment du piratage vraiment crapuleux (visant, par exemple, à s'emparer des codes d'une carte bleue), il ne faut pas exclure la pure curiosité ; ou le jeu, ou l'intention globale de nuire, mais sans intérêt pécunier.

    Diverses personnes et diverses institutions ont intérêt à connaître beaucoup de choses nous concernant. Y compris ce que nous considérons comme ne relevant que d'un cercle plus intime. C'est en particulier ce que nous destinons à des *happy few* sur les réseaux sociaux, et que d'autres parviennent à capter (soit en raison de maladresses de notre part, ou du manque de vigilance) qui doit être l'objet de toute notre attention.

514. Les réseaux sociaux constituent un ensemble de menaces importantes, pas seulement pour la personne qui s'y livre, mais également pour son entourage. Ce qui est évidemment bien plus grave encore, et très chargé d'enjeux juridiques. Ainsi, il est très facile d'identifier sur une photo un tiers, même si ce n'est pas fait de façon explicite, avec le nom mentionné. Or, cela peut nuire à ce tiers, aperçu sur une photo, même par hasard.

    Sans aucun doute, ce qui peut sembler anodin de prime abord, peut ne pas du tout l'être. En effet, une indiscrétion peut révéler qu'une personne ne se trouvait pas à l'endroit prévu à tel ou tel moment. Il peut y avoir suspicion - fondée ou non - d'infidélité conjugale, ou de faute professionnelle. Des compagnies d'assurances maladie peuvent, par exemple, arguer de telle ou telle photo qui fait foi pour dénier à quelqu'un des indemnités. Il n'y a guère de doute qu'elles cherchent à le faire, dans le but de faire elles-mêmes des économies. Le cas s'est posé au Québec. La salariée d'une entreprise, en arrêt maladie pour cause de dépression depuis un an, avait publié des photos qui auraient été prises dans un bar au cours d'un spectacle lors de vacances au soleil. Ce qui semblait mettre en doute la réalité de sa maladie.

D'une certaine façon, elle n'avait qu'à s'en prendre à elle-même, car poster de telles photos bien visibles était une imprudence.

515. Du point de vue juridique, le problème qui se pose, de plus en plus, est celui de la " divulgation " de faits (certes, faciles d'accès, mais) que la personne préférerait en général voir oubliés. Curieusement, ce qui peut être considéré comme relevant " du vu et du su de tout le monde " dans certains pays, ne l'est pas forcément dans un autre.

Cela vaut, par exemple, de l'âge du candidat. En France, il relève souvent de l'évidence - quoique de moins en moins désormais – d'indiquer, sur un CV, la date de naissance d'un candidat à l'embauche.

516. Il en va tout différemment aux Etats Unis, surtout pour un candidat appartenant, dit-on, à la classe protégée " des seniors ", à savoir des quarante ans et plus. La discrimination à l'embauche en fonction de l'âge est strictement interdite. On assiste parfois à des procès – qui peuvent d'ailleurs ne pas toujours être de bonne foi, à l'initiative d'avocats véreux – pour motif de suspicion de discrimination à cause de l'âge. Il est vrai que l'âge, au moins approximatif, peut souvent être plus ou moins déduit des autres informations d'un CV.

517. La question particulière du secret médical[384], singulièrement délicat, doit faire l'objet d'un développement à part. Il a bien entendu été créé pour protéger les personnes de toute discrimination en raison d'un problème de santé, et de la curiosité malsaine des uns et des autres. D'ailleurs, certaines maladies peuvent être considérées comme infamantes, comme le SIDA, ou des maladies vénériennes. Il n'est, en général, même pas possible à un patient de délier son médecin du secret professionnel. Pour deux raisons principalement. La première, tient aux risques de pressions que l'on pourrait exercer sur ce même patient, afin qu'il le fasse, par exemple un chantage à l'embauche. La seconde, évidemment très liée, est que cela ferait porter de façon quasi automatique un soupçon sur ceux qui ne le font pas. Ce qui reviendrait à supprimer indirectement, et sans doute assez rapidement, ledit secret.

[384] Pour le secret médical en France : *https://www.service-public.fr/particuliers/vosdroits/F34302.* Vaste bibliographie : Patrick VERSPIEREN, « Le secret médical et ses fondements », 2007 *: https://www.cairn.info/revue-laennec-2007-1-page-6.htm#;* Pierre VERDIER, « Secret médical et partage des informations » *: https://www.cairn.info/revue-journal-du-droit-des-jeunes-2007-9-page-8.htm.* Pour le problème posé parl'essor du numérique *:* Maximilien AMEGEE*, La cybersurveillance et le secret professionnel : paradoxes ou contradictions : https://www.droit-technologie.org/wp-content/uploads/2016/11/annexes/dossier/81-1.pdf*

c. ***Le droit à l'oubli***

518. Le droit à l'oubli[385], est l'héritier d'une longue histoire. Il traverse différents champs de l'espace législatif. Il fonde l'idée de « prescription ». Ce principe général du droit consistant à déterminer une durée au-delà de laquelle une action en justice - civile ou pénale - n'est plus recevable. Certes, il ne s'agit pas véritablement d'un oubli au sens propre. En effet, le délit en cause peut être rappelé, mais aucune poursuite ne peut plus être engagée à son sujet. Plus largement, il y a une autre forme de prescription non pénale, qui désigne une sorte d'extinction automatique des droits dans le temps en droit privé. Ainsi, les lois tombées de fait en désuétude ne sont pas de fait abolies.

519. En matière pénale, seuls des faits singulièrement graves ne peuvent pas faire l'objet d'une prescription, comme ceux qui tiennent du crime contre l'humanité. On tend - de plus en plus - à y associer des crimes sexuels singulièrement horribles comme des viols et meurtres pédophiles, jugés de plus en plus sévèrement dans notre société.

    Aujourd'hui, un droit est de plus en plus souvent revendiqué, dans le cadre du numérique : celui de faire disparaître des données sur un site, ou collectées par un organisme de façon inutile ou abusive. En France, la Commission nationale de l'informatique et des libertés, la CNIL, reconnaît un tel droit[386]. Toutefois, seulement à certaines conditions. Il faut ainsi que les données en question soient utilisées à des fins de prospection, ou ne soient pas (ou plus) nécessaires au regard des objectifs avancés initialement pour les collecter.

520. Bien entendu, la reconnaissance d'un tel droit s'impose de façon toute particulière dans certains cas bien précis. Par exemple, lorsque les données font l'objet d'un traitement, ou si elles sont piratées, ou si elles ont été collectées alors que la personne était encore mineure.

    Cependant, le droit à l'effacement des données n'est pas absolu. Il existe des cas-limites où il ne peut être invoqué. Il faut également tenir compte de l'exercice du droit à la liberté d'expression et d'information.

521. En ce qui concerne spécifiquement le domaine de la santé publique, la question s'avère particulièrement délicate. Il peut, ainsi, y avoir des cas où des données ont bien un intérêt pour tous : par exemple, lorsqu'il s'agit de découvrir un nouveau vaccin pour telle maladie, à partir

---

[385] HAL, *Droit à l'oubli : https://halshs.archives-ouvertes.fr/halshs-01223778/file/RAPPORT-FINAL-Droit-a-loubli-2015.pdf;* David DECHENAUD*, Le droit à l'oubli numérique. Données nominatives – approche comparée, Paris, Larcier, 2015.*

[386] https://www.cnil.fr/fr/le-droit-leffacement-supprimer-vos-donnees-en-ligne

de l'observation clinique d'un patient. Dans un tel cas, on peut estimer que l'intérêt général l'emporte sur l'intérêt particulier, même si cela reste discutable.

Le droit à l'effacement ne saurait entrer en concurrence avec le respect d'une obligation légale. Par exemple, en France, le délai de conservation d'une facture qui est de dix ans. Le droit à l'effacement peut également être refusé, lorsque l'utilisation des données s'avère importante à des fins d'archivage, ou de recherche scientifique ou historique. Ou encore, en vue de recherches statistiques. Même si, dans ce cas, c'est souvent moins probant. En effet, ce qui est d'ordre statistique exige moins - en général - des données précises concernant le particulier.

522. Il va de soi que l'effacement des données ne saurait davantage faire fi de l'exercice ou de la défense de droits en justice. Pour des raisons assez évidentes, qui tiennent à l'importance de leur conservation, l'effacement des données ne saurait constituer une pratique générale. Elle est simplement limité à certains cas particuliers.

Outre ce cas plus spécifique de l'effacement des données, il faut considérer celui de sa limitation ou d'une mise en suspens provisoire. Cela vaut, par exemple, lorsque l'exactitude des données à caractère personnel est contestée, ou lorsque se présente un éventuel caractère diffamatoire.

523. Pour l'instant, dans les Emirats, le droit à l'oubli se trouve encore à un état inchoatif. Il faut dire que son élaboration dans le détail n'est pas simple. Comme l'atteste d'ailleurs le temps qui a été nécessaire pour que les institutions européennes tranchent la question (à savoir pratiquement une vingtaine d'années, entre la Directive sur la protection des données en 1995 et la décision de la Cour de justice de l'Union européenne du 13 mai 2014, qui consacre finalement un droit à l'oubli dans toute l'Europe).

Après quatorze années de discussions, c'est en 2009 que la Secrétaire d'Etat chargée de la prospective et du développement de l'économie numérique du Gouvernement français, Nathalie Kosciusko-Morizet, a véritablement décidé de la légitimité de l'affirmation d'un droit à l'oubli numérique. Les 30 septembre et 13 octobre 2010, des Chartes du droit à l'oubli numérique ont été adoptées. Il n'est pas indifférent de savoir que ni Facebook ni Google ne les ont accepté. En effet, par cette charte, ces signataires s'engagent à trouver un moyen de pouvoir demander la modification ou la suppression de toute donnée personnelle qui pourrait avoir être publiée sur les réseaux.

524. La volonté politique manifestée alors par la France a certainement encouragé Viviane Reding (alors vice-présidente de la Commission européenne et Commissaire européenne à la justice

aux droits fondamentaux et à la citoyenneté) à s'engager en faveur d'une large reconnaissance d'un tel droit, dans un discours marquant prononcé le 30 novembre 2010.

525. En janvier 2012, la Commission Européenne a publié une proposition de régulation européenne pour la protection des données. Celle-ci a été ensuite reprise par le Parlement européen et le Conseil des ministres.

526. La bonne volonté ne suffit pas lorsque se posent des problèmes concrets. Parmi eux, il y a celle d'un fournisseur de services de moteur de recherche de données sur l'Internet. Qeu se passe-t-il lorsque celui-ci crée une succursale ou une filiale dont l'activité vise les habitants de cet Etat ?

    Google invoque ce casse-tête juridique. Selon lui, un fournisseur ne saurait en droit - ou en fait - remplir les obligations qui incombent seulement au responsable du traitement des données. Autrement dit, la déontologie du traitement de données ne s'applique pas, ou s'applique de façon douteuse au fournisseur. On peut bien entendu imaginer que des intérêts économiques soient en jeu, mais les textes officiels sont clairs à cet égard : en aucun cas de tels intérêts ne sauraient être mis en balance avec les droits importants des personnes.

527. Il semble évident que ce droit est gênant pour des moteurs de recherche de l'importance de Google. Celui-ci a fini par se soumettre aux décisions européennes, mais à reculons, en élaborant à l'intention de ses multiples usagers un formulaire.

    Comme on pouvait, du reste, s'y attendre de nombreuses demandes lui ont été communiquées. Les plus nombreuses ont été celles des Français ; qui étaient, par ailleurs, les premiers à revendiquer un tel droit. Suite aux demandes qui lui sont parvenues, Google a retiré environ 150.000 liens. Ce qui veut dire - concrètement - qu'une majorité de demandes, loin d'être jugée absurde, est considérée comme légitime.

528. Ce nombre, en soi important, de liens supprimés ne signifie cependant pas que Google accepte mieux désormais le principe en cause. Le célébrissime moteur de recherches est d'ailleurs condamné pour la première fois en France, pour avoir rejeté une demande de suppression d'un lien vers un article de 2006 du quotidien « le Parisien ». En outre, certains dénoncent le fait que Google enlève surtout des résultats de recherche dans les versions européennes (et non pas au niveau mondial). Ce qui limite l'étendue de l'effacement. Qui plus est, en général, les liens supprimés sont ceux qui mentionnent explicitement le nom de l'intéressé, non pas les autres. C'est ignorer la facilité avec laquelle certaines informations peuvent être retrouvées par

recoupement. Ainsi, il est facile de retrouver en quelques secondes le nom d'une personne exerçant une telle charge. L'effacement du nom entier au profit d'initiales authentiques ne constitue pas non plus une véritable garantie. Tout dépend du nombre de ceux qui ont les mêmes initiales et qui pourraient ainsi être identifiés. Parfois les initiales sont transparentes.

Google se défend, en arguant du fait que certaines entreprises demandent que soient effacées certaines informations pour des raisons aucunement légitimes, mais dans une perspective de concurrence, pour désavantager des concurrents.

529. Dans une importante tribune, en date du 11 juillet 2014, David Drummond, alors avocat de Google, a rappelé que, sur ce sujet, il est fort difficile d'élaborer des critères très précis. Il semble indispensable de mener un débat sur cette question. Il souhaite la mise en place d'un comité consultatif, afin de déterminer les principes à suivre dans tel ou tel cas. Des problèmes délicats et aux contours indécis peuvent et doivent être posés : comme celui de savoir quelle est la nature et la délimitation exacte de la notion de droit à la vie privée pour une personne publique.

530. Il semble bien que nous soyons sur cette question en présence d'une sorte de conflits de devoirs, et donc de droits. Comment trouver un juste équilibre entre le droit à l'oubli et celui à l'information et à la liberté d'expression. Il faut ainsi savoir que la *Wikimedia Foundation,* l'hébergeur de Wikipédia, dont des articles sont concernés par le droit à l'oubli imposé à Google, lance une accusation contre certaines décisions comme celle de « perforer l'accès au savoir ». Jimmy Wales, le cofondateur de Wikipédia, va jusqu'à fustiger une loi complètement folle. Il est vrai que, dans un tel débat, il est à la fois juge et partie.

531. En réalité, en vertu d'une tradition - tout anglo-saxonne du reste, on peut imaginer que c'est la jurisprudence qui l'emportera sur des lois ou des décrets. Il est donc intéressant pour les Emirats d'étudier les décisions judiciaires qui ont été prises dans d'autres pays. Par exemple, celles relatives au cas d'une chirurgienne hollandaise qui a remporté son combat face à Google en 2018. Elle avait été, au départ, suspendue par l'ordre des médecins avant d'être réintégrée et blanchie. Or, sur le net, se trouvait encore une mention de la sanction. Ce médecin demanda donc à Google d'effacer tout ce qui mentionnait une sanction. En effet, beaucoup ne retiennent qu'une chose sur l'Internet et non tout ce qui est écrit (même si c'est parfois le plus important et le plus récent).

532. Il est fort instructif à cet égard de considérer tout ce qui pouvait motiver cette demande. Dans le cas particulier d'un acte chirurgical, la mauvaise réputation ou le soupçon de dangerosité prennent d'emblée une dimension considérable. En effet, il est évident que personne ne veut courir le risque létal d'être opéré par un chirurgien douteux. On peut donc comprendre la détermination de la chirurgienne hollandaise à vouloir faire disparaître les données la concernant. Elle dépose plainte, mais se heurte à l'incompréhension de Google. Celui-ci estime que les informations contenues relèvent du domaine public et de l'intérêt légitime des personnes qui doivent pouvoir bénéficier de tous les renseignements concernant les médecins (surtout avant d'être opérées) en raison de risques graves. Finalement, la décision de justice privilégie l'intérêt supérieur de la chirurgienne à ce que « son nom ne soit pas instantanément associé à une liste noire de docteurs à chaque fois que son nom est tapé dans Google ». La décision judiciaire aurait certainement été différente si la responsabilité de la chirurgienne avait été avérée. Si la sanction contre elle avait été maintenue.

533. La France est décidément en pointe sur cette question. C'est dans ce pays que, le 13 octobre 2010, a été mise en place une Charte du droit à l'oubli numérique à l'initiative de la Secrétaire d'État à l'Économie Numérique, Nathalie Kosciusko-Morizet. Ceci, dans le but de renforcer la protection de la vie privée sur l'Internet et de simplifier et de faciliter la suppression et la désindexation de données personnelles publiées.

534. Un autre sujet d'inquiétudes est celui de la durée de conservation des données, qui est longue, et qui semble donc pénaliser les personnes, même si l'intérêt de l'information demeure. Dans tous les systèmes juridiques, la prescription exprime une sorte de droit à l'oubli pour des fautes passées[387]. Comme l'écrivait récemment dans un article du monde Anne Chemin, « une société sans oubli est une société tyrannique »[388]. Par ailleurs, la mémoire de l'opinion est fortement évanescente. En principe, un sujet d'information fait rapidement place à un autre et est oublié. Toutefois, l'inscription sur le net le rappelle et empêche ce processus d'oubli Parmi les points très problématiques, un autre doit être mentionné. Dans de nombreux sites, il n'est pas possible à un internaute de récupérer ses données personnelles, dans la mesure où il s'est désinscrit dudit service. Ce qui le prive d'un droit et d'une protection qui doivent être reconnus en réalité à tout consommateur.

---

[387] Patrice JOURDAIN et Patrick WERY*, La prescription extinctive - Études de droit comparé*, Louvain, Bruylant, 2010 ;

[388] *https://www.lemonde.fr/idees/article/2020/01/10/la-prescription-ou-les-limites-de-l-oubli_6025372_3232.html*

535. Par ailleurs, l'une des questions les plus urgentes à traiter est bien celle de la manière dont il est possible et nécessaire de protéger des données personnelles d'un point de vue juridique. Ce qui nous conduit à envisager l'hypothèse de leur patrimonialisation. Ce qui concerne - en définitive - tout individu revêt une prégnance singulière dans le contexte du monde du travail (des droits et devoirs des partenaires qui y sont impliqués).

Chapitre II : Données personnelles et vie collective

***Section* I *: La patrimonialisation des données personnelles*.**

536. En matière de droit autour de l'usage et de l'analyse des données personnelles, le respect de la loi ne suffit pas toujours. En effet, il arrive que la loi soit en retard par rapport aux technologies. Une entreprise doit anticiper l'impact de ses actions et parfois s'auto-censurer. L'indécision peut aussi créer une sorte de stress avec des effets inhibants.

Plus fondamentalement peut-être, le droit a pour vocation d'encadrer de la façon la plus rigoureuse possible (mais certainement non-unique et non-exclusive) des pratiques qui le précèdent. Qui, de toute façon, lui échappent en partie.

537. Autrement dit, sa mission s'avère à la fois plus ambitieuse et plus modeste. D'une part, il lui revient de donner toute sa place au bon sens et au discernement éthique et responsable ; qui est celui des individus comme des entreprises, face à une décision à prendre (de conservation ou non de données), de diffusion ou de réserve. En ce sens, le droit ne devrait pas limiter l'activité indépendante des individus et le discernement délicat, mais au contraire à la fois les situer et les susciter. Le droit ne peut, bien entendu, pas prévoir toutes les circonstances qui orientent une décision. S'il se veut trop précis, il risque de tout bloquer et de s'enfermer dans des impasses. « Trop de loi tue la loi » nous enseignait déjà Montesquieu . En même temps, le droit doit quelquefois être complété par des décisions prises - à petites échelles, sur le terrain, dans un contexte bien particulier et, qui plus est, mouvant.

a. *La donnée, propriété de la personne*.

538. En réalité, il apparaît de plus en plus que la solution serait de faire de la donnée une véritable propriété de la personne concernée. En principe, pour être considérée comme la propriété d'une personne physique, il faut que la chose soit extérieure à cette personne : ne soit pas une partie de son corps, ou un élément de la personne comme sa psychologie ou un secret la concernant.

C'est pour cela du reste qu'une partie du corps n'est pas commercialisable, à l'opposé d'abominables pratiques du XVIIIe et du XIX, au cours desquelles on vendait sur le marché des cheveux ou des dents cédés par des pauvres pour survivre : une horreur que dénonce par exemple Victor Hugo dans ses célèbres « Misérables » . Du reste, mais ce point ne peut être développé ici, la réticence qui existe à l'endroit d'une légitimation de la prostitution comme

d'une pratique acceptable et encadrée tient souvent à la commercialisation du corps qu'elle exprime, même si le problème est certainement fort complexe.

En tous les cas, une donnée personnelle semble ne pas pouvoir relever du bien possédé. En effet, elle constitue une information en quelque sorte intrinsèquement liée à la personne. Elle est presque comme une partie de son corps. On peut aussi voir en la donnée personnelle quelque chose qui appartient à la sphère privée. Or, justement, même si c'est paradoxal, lorsqu'il s'agit de ce qui relève des objets de la sphère privée, c'est en général le droit de propriété qui le protège le plus efficacement.

539. L'une des solutions avancées pour préserver les données serait d'en faire non plus une qualité essentielle, mais quelque chose qui leur appartiendrait. Autrement dit, de les faire entrer dans la catégorie de la propriété. Cette idée est défendue en particulier par le jeune penseur libéral Gaspard Koenig, qui défend également l'hypothèse d'un revenu universel pour tous[389] ou une conception nouvelle du rôle de l'Etat (qui ne limiterait pas l'indépendance des individus mais au contraire contribuerait à la leur garantir, dans le monde marqué par les révolutions technologiques[390]). En pleine cohérence avec sa vision libérale, il défend à présent l'idée d'un système de propriété privée des données personnelles[391].

Ce qui implique aussi que chacun puisse vendre ses propres données personnelles, qui ne seraient donc plus à considérer comme une extension de son corps. Ce dernier point peut être considéré comme le plus choquant, pour celui qui refuse de faire des données personnelles un bien possédé. D'une certaine façon, la solution de Gaspard Koenig présente l'avantage de la simplicité. Chacun serait totalement maître de la destination de ses données, au moins en droit.

540. Tout abus serait alors considéré comme un vol très grave, à savoir si une autre personne physique ou une personne morale s'emparait de ces mêmes données. Yuval Noah Harari, essayiste israélien très populaire, qui envisage un tournant profond et radical de l'humanité, pense - quant à lui - que la possession et la collection des données personnelles est la question politique la plus importante de notre temps[392]. Dans un même esprit libéral, il partage le point de vue de Gaspard Koenig selon lequel l'individu devrait pouvoir choisir, s'il le souhaite, de vendre ses données personnelles à l'entreprise de son choix. Cela pourrait lui permettrait de

[389] Gaspard KOENIG, *Liber. Un revenu de liberté pour tous*, Paris, éditions de l'onde, 2015
[390] Gaspard KOENIG*, Le révolutionnaire, l'expert et le geek*, Paris, Plon, 2016.
[391] *https://www.generationlibre.eu/medias/propriete-des-donnees-personnelles-koenig-harari/*
[392] Yuval Noah HARARI, *Homo Deus. Une brève histoire du futur,* Paris, Albin Michel, 2017.

s'enrichir et empêcherait (en tous les cas, en amont) que l'on puisse s'emparer de ses données personnelles. Il pourrait, par exemple, avoir des parts de marché dans l'entreprise de recherche à laquelle il l'offre. On peut même se demander si cette possibilité de chacun de vendre chèrement ses propres données – ou de faire des investissements ce qui est évidemment plus judicieux – ne pourrait pas constituer une sorte d'alternative au revenu universel d'activité.

541. D'une certaine manière, nos données personnelles ne sont-elles pas nos actifs les plus importants et les plus disponibles, ou ne vont-elles pas le devenir ? Cette possibilité pour chacun de vendre ses propres données personnelles s'inscrirait aussi dans une cohérence « gagnant/gagnant ". Elle serait également avantageuse pour les autres. Par exemple, par le biais de la formation d'une coalition des intérêts des pays exportateurs de données. Ce qui pourrait être souvent, en l'occurrence, le cas des pays plus pauvres et plus défavorisés qui rattraperaient ainsi leur retard.

Sans cette reconnaissance d'une vraie possession par chacun de ses propres données, il y a en effet le risque d'une forme de néo-colonialisme numérique : les pays avancées en la matière contrôlant et dominant les données des autres pays. Comme jadis les plus puissants se livraient à l'extorsion des matières premières, dorénavant les plus avantagés risquent de se livrer à l'extorsion de l' « or numérique » si l'on peut dire : à savoir, les données des personnes vivant dans des pays plus pauvres.

542. Il est évident que cela exigerait de trouver une structure légale, qui préserverait le droit de propriété des individus sur leurs données. Un peu à l'exemple de ce qui constitue la propriété intellectuelle. Cela pourrait être - pourquoi pas – la création de syndicats de propriétaires de données, contrôlant avec vigilance la négociation des individus avec Amazon, Ali Baba et autres GAFAM. Si aujourd'hui les individus se sentent en infériorité, et démunis face à de tels géants disposants de personnes compétentes, expertes et retorses, alors qu'eux-mêmes sont dépourvus des connaissances et de la ruse nécessaires, ce ne serait plus le cas alors. Dans la mesure où de tels syndicats pourraient devenir très vite riches et puissants, et ainsi se doter de juristes très au fait et aux compétences pointues. L'idée semble donc défendable et parfois opportune d'affirmer que leurs données appartiennent aux individus comme leur propriété[393]. Si l'on suit cette logique, cela renforcerait leur droit de ne pas se les voir dérober par quelqu'un d'autre.

[393] Arnaud ANCIAUX et Joëlle FARCHY, « Données personnelles et droit de propriété. Quatre chantiers et un enterrement » in *Revue internationale de droit économique*, 2015, 3, 307-331.

543. Du reste, faire des données une propriété favorise certainement la régulation des conflits qui peuvent apparaître les concernant. Ceci, dans la mesure où une telle catégorie juridique implique un cadre (avec des droits et des devoirs) qui lui sont associés, mais aussi des moyens de recours tout-à-fait spécifiques. On peut, en effet, imaginer que les données personnelles se trouvent mieux protégées : dans la mesure où elles entrent dans la catégorie d'un bien possédé plutôt que dans celle d'un contrat établi. En effet, dans ce dernier cas, sauf précisions contraires apportées, il s'agit en général de concéder une collection et une utilisation des données en échange d'un avantage octroyé comme par exemple l'accès à une plate-forme.

544. On peut estimer que la garantie apportée est minimale. D'une certaine façon, le cadre contractuel est loin de véritablement souligner les droits de la personne à protéger ses propres données. Il semble plutôt inciter à la cession de ce droit, moyennant - il est vrai - un avantage en contrepartie.

    Toutefois, c'est précisément cet avantage qui semble constituer un certain danger. Dans la mesure où il peut aveugler les personnes sur l'autre aspect du contrat (qui n'est plus à leur bénéfice cette fois) : celui de les persuader de se priver un peu vite de protections pourtant importantes. Les garanties offertes dans le cadre d'un contrat peuvent sans doute être bien réelles, mais le contexte dans lequel elles sont placées donne le sentiment d'une incitation à la cession des données, même limitée ; d'une moindre insistance accordée à la protection des individus. Il semble ne pas s'agir d'une simple nuance.

545. Dans le cadre d'un contrat, la protection des données personnelles semble plus concédée qu'affirmée. Elle demeure en principe assurée, mais sur le mode d'une exigence qui passe au second plan : que l'on continue à poser et à respecter – au moins en théorie, mais qui n'est pas soulignée comme exigence et d'une importance vitale.

    Dans le cadre du recours à la propriété des données personnelles, on assiste à une sorte de renversement de priorité par rapport à la tendance actuelle : en faveur des individus et du contrôle libre et éclairé qu'ils doivent absolument pouvoir garder de ce qui les touche de plus près (et souvent le plus profondément).

546. Le recours à la propriété des données personnelles semble donc pouvoir bien servir l'intérêt des individus. Il leur garantit une meilleure maîtrise, moins vulnérable, de leurs données et de leur vie privée. En outre, les individus peuvent jouir plus facilement encore de la possibilité d'en tirer profit.

547. Pour autant, les entreprises et institutions ne sont pas perdantes, alors même que l'accès qu'elles peuvent avoir aux données se trouve limité. En effet, cette limitation s'accompagne par compensation d'une amélioration qualitative de ce qui est recueilli. Or, cette amélioration va bien entendu dans leur intérêt. En effet, cela ne leur sert pas véritablement d'avoir des données nombreuses, mais de mauvaise qualité ou peu fiables. La confiance doit régner entre l'individu dont les données sont recueillies – ou protégées – et les institutions. Ceci, afin que chacun sorte gagnant d'un processus qui ne saurait traduire une rivalité d'intérêt.

548. On pourrait parler d'une amélioration du traitement des données dans un sens gagnant/gagnant. En France, par exemple, il faut savoir que la propriété ne peut s'appliquer qu'à la création intellectuelle de ces données, comme dans le cas du droit d'auteur ou d'un brevet de découverte et non aux données elles-mêmes. Les personnes physiques bénéficient bien entendu de droits, mais il ne s'agit pas d'un droit de propriété, mais d'un droit de protection. Ce qui est différent, et doit à chaque fois être clairement précisé et délimité, comme le droit à l'image, à la voix et à la protection de la vie privée.

    C'est pourquoi, dans une même logique, la protection des données personnelles est garantie par la loi du 6 janvier 1978 et par la directive 95/46/CE s'inscrit rigoureusement dans une perspective de défense des droits attachés à l'individu.

549. Une telle patrimonialisation implique que l'individu doive pouvoir monétiser ses propres données ; devenir – si l'on peut dire – son propre trader[394]. Or, cette idée suscite une certaine répugnance. On y voit comme une réification des données personnelles dont l'individu pourrait faire un commerce, même si c'est à son propre bénéfice[395]. En d'autres termes, l'individu jouit de l'usufruit de ce qui le constitue en propre mais ne saurait en être propriétaire[396]. À la base d'une telle conception de la protection des données se trouve certainement le principe de finalité déterminée.

550. Dans un Rapport important rendu en avril 2017 par le Conseil National du Numérique l'idée de patrimonialisation est rejetée à cause des difficultés à déterminer ce qu'est exactement une

[394] Alain BENSOIUSSAN, « Chacun va devenir le trader de ses données personnelles » in *Archima*g, 274, mai 2014, 12.
[395] Nicolas OCHOA, « Pour en finir avec l'idée de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », in *Revue Française de droit administratif*, 2015, 1157.
[396] Pierre TRUCHE, Jean-Paul FAUGERE, Patrice FLICHY, « Administration électronique et protection des données personnelles : Livre blanc », in *La Documentation française,* février 2002 : *https://www.ladocumentationfrancaise.fr/rapports-publics/024000100/index.shtml*

donnée personnelle. Or, il n'est pas possible de patrimonialiser une réalité aux contours flous et mouvants. Toutefois, derrière cet argument discutable (car en définitive il n'est pas si difficile que cela de définir précisément une donnée, même si le choix de cette définition se révèle en bonne part arbitraire) se dissimule un débat de fond ; que l'on peut qualifier d'idéologique. Un courant de tendance libérale affichée, comme le *think-tank* libéral *Génération Libr*e, présidé par l'essayiste Gaspard Koenig cité plus haut, est bien entendu favorable à la patrimonialisation par chacun de ses propres données personnelles. Ce qui d'ailleurs lui permettrait d'en tirer un profit pécunier[397] . Néanmoins, ce point de vue est jugé presque immoral par d'autres. Pourtant, il y a bien quelque chose d'alléchant dans cette résistance à la mainmise des plus puissants, des GAFAM, sur ce qui nous concerne. Sur cette nouvelle possibilité, ainsi créée, de s'enrichir en définitive très facilement. En effet, nous produisons presque constamment des données numériques ; pour peu que nous ne soyons pas déconnectés du monde numérique. Nous en produirons certainement de plus en plus. Alors pourquoi ne pas transformer un risque et une sorte d'évidence spontanée en une occasion heureuse de créer de la richesse pour soi, mais aussi pour les autres et la société toute entière ?

b. <u>La commercialisation des données en question</u>

551. Faire passer la protection de la donnée personnelle, de l'ordre des droits fondamentaux à celui du contrat commercial, paraît, à tort ou à raison, les galvauder[398]. D'autant plus qu'appliquer les règles du domaine professionnel revient *ipso facto* à se passer de la protection juridique accordée aux personnes physiques, qui - pour imparfaite qu'elle puisse être en l'état actuel des choses - représente néanmoins une garantie plus fondamentale que celles apportées par les clauses dans un cadre mercantile.

Plus concrètement, des plateformes - jusqu'alors gratuites - pourraient bien désormais monnayer leurs services, pour compenser les frais que leur causerait l'acquisition de données désormais susceptibles d'être achetées.

---

[397] GENERATION LIBRE, Rapport Mes données sont à moi : *https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf*. Dans un sens analogue Tribune Nos « données personnelles nous appartiennent ! Monétisons-les in *Le Monde*, 05 février, 2018.
[398] Réflexions critiques en ce sens (entre autres) : Nicolas MAZZUCCHI, « Les données sont-elles une marchandise comme les autres » in *Fondation pour la recherche stratégique*, 26 juillet 2018 : *https://www.frstrategie.org/publications/notes/les-donnees-sont-elles-une-marchandise-comme-les-autres-12-2018*

Ainsi, ce que gagnerait d'un côté le citoyen lambda (grâce à ses données) serait d'un autre côté reperdu par lui. Pour rester connecté, il devrait en définitive s'acquitter d'un paiement sensiblement égal à ce qu'il aurait touché. Ainsi, nous serions en présence d'un jeu à somme nulle en quelque sorte. L'argent gagné serait reperdu. Les grandes plateformes tireraient habilement leur épingle du jeu. Un tel scénario n'est pas à prendre à la légère. Ceci, d'autant plus qu'un bras-de-fer entre des puissants et des individus lambda tournerait largement au désavantage de ces derniers. Ceci, d'autant plus qu'ils seraient vulnérables du fait d'avoir renoncé à une protection juridique essentielle, au profit d'une stratégie mercantile. On peut en effet concevoir que peu d'internautes seront en mesure de revendiquer une rémunération autre que symbolique. D'autant plus la valeur marchande des données (surtout de certaines d'entre elles) n'est guère facile à établir.

552. Assez facilement, une plate-forme pourrait obtenir gratuitement des données en faisant miroiter de son côté la gratuité de l'accès présentée comme une faveur avantageuse. Ce faisant, elle renforcerait encore sa mainmise sur ce qui relève du plus personnel. À l'évidence, cela fait peser de grands risques ; aussi bien pour les libertés individuelles, que pour le respect de la vie privée, sans oublier le droit à l'oubli.

553. Du reste, de façon peut être paradoxale, une telle patrimonialisation ne favoriserait peut-être pas non plus, au bout du compte, la libre circulation numérique. Elle pourrait, en réaction, induire une posture de repli et de conservation frileuse des données. On sait combien – et à quelle vitesse – les grandes entreprises numériques se sont développées grandement dans l'Union Européenne, au début des années 2000, ou au milieu de cette décennie, pour Facebook, LinkedIn (désormais Microsoft), Twitter et bien d'autres.

    Cette déferlante a pris tout le monde de court, en particulier les juristes. On peut parler d'une situation totalement inédite, qui ne permet plus de protéger les données personnelles ni de respecter la vie privée ; quelles que puissent être par ailleurs les déclarations d'intention.

554. Le montant des sanctions que peuvent prononcer les autorités de contrôle européennes, à savoir les différents CNIL européennes, reste limité. Ce qui en relativise la portée, quand on considère - par ailleurs - les moyens financiers considérables des géants du numérique. Les sanctions, à supposer déjà qu'elles soient appliquées, n'ont donc plus de caractère dissuasif. Celui-ci se trouve neutralisé d'emblée par l'insuffisance des sommes demandées.

555. Au cours de l'été 2017, les sociétés Facebook Inc. et Facebook Ireland ont été condamnées au maximum de la sanction prévue, à savoir 150.000 euros, pour les combinaisons de données

qu'elles ont effectuées à des fins de ciblage publicitaire (après le rachat de la messagerie instantanée WhatsApp, sans le consentement des abonnés de la messagerie). Cette somme peut paraître considérable, mais en réalité elle est plutôt dérisoire pour les sociétés concernées - en considération de leurs gains et leur richesse.

Il faut, du reste, déplorer l'inaction des pouvoirs publics européens qui ont failli dans leur rôle de protection de leurs citoyens. D'autres menaces sont certainement perçues, à tort ou à raison, comme plus urgentes : à savoir le terrorisme ou le harcèlement sexuel dont les réseaux sociaux font d'ailleurs leur miel.

556. Il est vrai également que de nombreux pays, et singulièrement la France, manquent considérablement de moyens pour relever les défis qui s'imposent en matière de justice. eaucoup de magistrats demeurent perplexes et insuffisamment formés face à de nouveaux enjeux, plus complexes et inattendus. Le consommateur de base est de toute façon totalement déboussolé face à un système dont il ne prend que difficilement conscience de la perversité. Par exemple, il est sommé de lire des conditions d'utilisation qu'il ne lit jamais. Ou encore, de telles conditions d'utilisation peuvent soumettre le contrat à un droit et à un juge qui n'est pas européen. Elles peuvent également contraindre le consommateur à conclure un contrat avec la société mère du prestataire de service. De sorte que le malheureux citoyen se trouve concrètement paralysé face à une situation qui le dépasse et dans laquelle il a été piégé.

Sans doute, il ne s'agit aucunement en soi d'une situation de non-droit, mais plutôt d'une paralysie du droit qui ne peut être appliqué ; dont l'exercice est bridé, et ce très habilement. De sorte que tout recours devient impossible ou du moins fort difficile.

557. Des progrès récents peuvent être constatés. Ainsi, le 25 mai 2018 a vu l'entrée en vigueur d'un Règlement Européen[399] dans les 28 Etats de l'Union. Celui-ci donne aux CNIL Européennes un pouvoir de sanction bien supérieur. Il peut atteindre 4% du chiffre d'affaires mondial total du contrevenant. La sanction n'est donc plus dérisoire, mais elle n'est peut-être pas pour autant véritablement efficace, du moins autant qu'il le faudrait.

Chaque Etat peut également mettre en place une action de groupe en matière de données personnelles. De nouveaux éléments permettent d'espérer une protection plus solide de la personne et de ses données personnelles, sans passer par la patrimonialisation. On peut penser

[399] *https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels*

que, dans des délais relativement raisonnables, le droit personnel de l'individu à protéger ses données personnelles lui sera enfin vraiment reconnu.

558. Le consentement éclairé de la personne deviendra l'axe de toute la protection juridique. Ceci implique un accès facile et permanent, par chaque personne - qui ne doit aucunement en être dissuadée, à une base de données pour vérifier si elle y figure ou non. Ceci, afin qu'elle puisse corriger certaines données fausses ou inopportunes ; voire même pour qu'elle refuse de figurer dans cette base de données. Toutefois, la garantie n'est véritablement solide que si la personne jouit, à tout moment, et pour toutes les données du droit de retirer son consentement, sans qu'il n'y ait de justification à avancer, simplement par choix personnel.

559. Il semble nécessaire qu'un tel droit lui soit reconnu, un droit absolu et fondamental, un droit que rien ne peut occulter. Telle semble être l'une des deux options pour protéger les données et les personnes : l'alternative à celle de la patrimonialisation des données, évoquée plus haut. En effet, cette dernière présente tout de même un inconvénient de taille et de fond, indépendamment de risques plus conjoncturels. Si les données personnelles sont considérées comme des biens possédés (que l'on peut vendre), il n'est plus possible de revenir sur le consentement accordé. Puisqu'il y eut une cession de type commercial. Qui cède une donnée, ne peut en récupérer la propriété. Toute imprudence peut alors s'avérer lourde de conséquences. Or, nous avons déjà signalé la vulnérabilité des personnes physiques face à certaines stratégies adroitement mises au point.

560. D'un point de vue juridique plus fondamental on peut se demander encore si le problème n'est pas celui de la nature spécifique des données, qui se situerait en quelque sorte entre la personne et la chose[400]. En définitive, une donnée personnelle ne serait pas tant une réalité floue (comme on le dit quelquefois à tort), mais de façon plus complexe et plus subtile une réalité qui relève en quelque sorte de deux ordres de réalité, sans s'inscrire vraiment dans l'un d'entre eux ; qui flotte un peu entre les deux.

561. On pourrait même dire qu'une donnée personnelle relèverait à la fois de l'être et de l'avoir, sans qu'aucune de ces catégories ne lui corresponde vraiment. Elles ne sont pas des personnes, mais sont inhérentes à des personnes. Elles constituent des informations qui peuvent circuler librement, à l'insu des personnes, et se détacher des personnes. Elles ne sont pas comme les membres d'une personne, par exemple son cœur ou sa jambe. Ce sont des réalités abstraites et

[400] Philippe MOURON, « Pour ou contre la patrimonialité des données personnelles » : *https://hal-amu.archives-ouvertes.fr/hal-01823901*

intellectuelles. Pourtant elles participent de la personnalité des personnes physiques, parfois la plus intime. Le choix de la patrimonialisation (ou son refus) pourrait bien tenir à la conception que l'on privilégie : soit celle d'une donnée comme penchant du côté de la personne physique, soit d'une donnée comme penchant du côté de la chose.

562. Les choses sont certainement plus complexes. Le choix ou le refus de la patrimonialisation ne relèvent pas d'abord d'une démarche déductive. Autrement dit, ce n'est pas en s'appuyant sur la détermination de la nature exacte de la donnée personnelle que se fonde telle ou telle approche (visant à en garantir la protection), mais à partir d'une intuition globale du problème et de ses enjeux, précisément en raison non d'un flou mais du caractère singulier et hybride de la notion de donnée personnelle.

En effet aucune des deux positions au sujet de la patrimonialisation ne tranche véritablement la question de façon nette et péremptoire. On parle d'une commercialité « limitée » de la donnée personnelle. Ce qui veut bien dire que nous ne sommes pas en présence d'un objet qui serait commercialisable - comme les autres, mais d'une réalité différente pour laquelle en définitive on concèderait la possibilité d'être commercialisé (plus qu'on ne la lui reconnaîtrait véritablement). La patrimonialité des données relèverait de règles spéciales et spécifiques.

563. On peut penser, par ailleurs, que les tenants d'une patrimonialisation des données personnelles participent davantage d'une approche réaliste et pragmatique. Leur argumentaire souligne surtout la situation de fait, indépendamment des principes idéaux. De fait, l'insistance sur la protection des données personnelles et de l'intégrité de l'individu, ainsi que de sa dignité semble *in concreto* moins efficace qu'une stratégie à court terme, qui inclut la patrimonialisation.

En revanche, les opposants à la possibilité d'une patrimonialisation se fondent aussi sur des risques concrets qu'ils mettent en évidence et soulignent. Ils accentuent également l'enjeu philosophique. Ils cultivent une approche plus essentialiste pourrait-on dire, qui dégage une nature humaine à protéger ; au-delà de toute préoccupation pragmatique (et a fortiori mercantile).

564. Les droits de la personnalité[401], qui poursuivent et prolongent ceux de la personne, sont toujours envisagés sous un angle d'approche un peu spécifique et un peu différent ; moins direct que lorsqu'il s'agit des droits de la personne physique elle-même. Cela est, par exemple, le cas du droit à l'image, l'un des premiers.

[401] Bertrand BEIGNIER*, Le droit de la personnalité*, Paris, PUF, Que sais-je, 1992 ; André BERTRAND, *Le droit d'auteur et les droits voisins,* Paris, Masson, 1991.

565. L'image d'une personne n'est pas exactement cette personne elle-même, de sorte que l'on peut la situer aussi entre la personne et la chose. Ceci, d'autant plus que l'image peut se monnayer, parfois de façon très chère. Depuis que la photographie existe, l'image d'une personne se détache - en quelque sorte - d'elle-même pour devenir une sorte de chose. Il n'en allait pas exactement de même lorsqu'un peintre sur une toile représente quelqu'un. La représentation n'est pas véritablement l'image photographique. Il faut souligner que malgré son caractère spécifique le droit à l'image fait bien l'objet de contrats d'exploitation et génère des revenus. Cela est vrai également du droit au nom. Ce qui veut simplement dire que même si les droits de la personnalité demeurent en principe extrapatrimoniaux (par voie de conséquence, incessibles, insaisissables et intransmissibles), cela n'empêche pas de faire des concessions pratiques ; d'admettre une certaine forme de patrimonialisation, certes limitée et encadrée, mais réelle.

Le problème ne se pose donc pas de façon dichotomique et tranchée. Un compromis bien pesé demeure envisageable.

c. Données personnelles et œuvres de l'esprit

566. Pour éclairer le débat sur l'éventuelle patrimonialisation des données personnelles, il est également fructueux de les rapprocher de ce que l'on appelle les œuvres de l'esprit : du droit d'auteur. Il convient de se référer à la personnalité de celui qui s'exprime, même s'il s'agit d'une fiction et non d'une autobiographie par exemple.

567. La nature juridique du droit d'auteur s'avère également difficile à cerner. Incontestablement une œuvre de l'esprit, un tableau ou un livre, extériorise quelque chose de la personnalité de l'auteur avec laquelle elle ne se confond jamais totalement, mais avec laquelle elle continue pourtant à entretenir un lien constitutif interne. On peut encore aller plus loin et noter que certains éléments de l'identité d'une personne peuvent quelquefois faire l'objet d'une mise en forme originale, dans des jeux vidéo et sur les réseaux sociaux. Ils deviennent ainsi des éléments d'un personnage de fiction. Des données personnelles sont alors mêlées à ce qui relève de la pure création. On peut se demander si le fait de reconnaître une certaine « transportabilité » des données, par exemple (qui découle du droit de les transférer d'un service à un autre), n'est pas en soi une forme de réification des données et de la personnalité. Celle-ci accorderait un droit supplémentaire et une protection à la personnalité et à la personne physique.

Ainsi, la chosification des données ne se réalise pas forcément, en soi, au détriment, de la liberté personnelle et d'une vision idéale de la personne libre. On peut également penser à la création, en droit français, d'un droit sur le sort *post mortem* des données. Ce qui laisse entendre une possible transmission de celles-ci aux héritiers. Cette ouverture demeure cependant incertaine et limitée. En effet, la même loi française rappelle que les droits ouverts par la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 disparaissaient au moment du décès du titulaire.

568. Outre la matérialité d'une loi, ou d'une décision, il y a, bien entendu, son interprétation. Parfois, on a pu subodorer une reconnaissance implicite (ou inchoative) de la patrimonialité de fichiers de données personnelles. Cela vaut par exemple avec l'arrêt de la Chambre commerciale de la Cour de cassation, en date du 25 juin 2013, dans lequel il est confirmé qu'un fichier de clientèle informatisé non déclaré à la CNIL constituait une chose hors commerce et ne pouvait valablement faire l'objet d'une cession. Or, une telle formulation, paradoxalement, sous-entend également que le fichier puisse faire l'objet d'une exploitation. En tous les cas, elle envisage cette possibilité.

569. Il peut également sembler intéressant de souligner que l'article 544 du Code civil français[402] délimite un droit de propriété, indéfini dans son contenu, mais non illimité dans sa portée. Ainsi, certains actes peuvent-ils être interdits au propriétaire, soit en raison de la nature des biens en cause, soit en raison de restrictions légales. C'est pourquoi, la patrimonialisation des données personnelles ne signifie en rien l'absence de toute barrière et de toute protection. Ce n'est pas une porte ouverte à tous les abus et excès.

Du reste, la libre disposition des données personnelles serait exclue quant à certaines données qui se présenteraient comme les plus sensibles, telles celles touchant à l'intimité et à la dignité des personnes. Ainsi, le règlement général et les autres textes relatifs à la protection des données personnelles peuvent-ils être considérés comme exprimant justement des restrictions légales ? Dans la mesure où elles conditionnent l'exercice du droit de propriété sur ces données.

[402] Cet article fort important rappelle les trois éléments classiques du droit de propriété : l'*usu*s, le *fructus* et l'*abusus*. Des limitations sont introduites dans le droit de propriété par les interdictions posées dans « les lois et les règlements ». En clair, il s'agit pour le propriétaire de respecter l'ordre public et l'intérêt général. Et on pourrait dire aussi une certaine dimension morale. En tout cas, et c'est cela le point essentiel, le propriétaire n'est donc pas « maître absolu » de ses biens, il se heurte à certaines restrictions et interdictions. *https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006428859&cidTexte=LEGITEXT000006070721*

570. En effet, les deux conceptions souvent opposées ne sont peut-être pas totalement contradictoires. Elles pourraient - sans doute - faire l'objet d'une certaine harmonisation, réconciliation. Elles relèveraient davantage d'une question de point de vue que d'une alternative abrupte et définitive. De sorte que le législateur pourrait naviguer entre elles avec une certaine latitude. Ceci, ne veut évidemment pas dire que, pour autant, la patrimonialisation ne puisse pas susciter un certain nombre de réserves.

Très concrètement, la mercantilisation des données suppose - tout de même - qu'il soit intéressant de faire une collecte forcément onéreuse ; donc que les données présentent un intérêt assez grand pour un tel[403]. Or, cela risque de susciter un effet pervers collatéral. En effet, les plates-formes vont chercher à atteindre un seuil de rentabilité maximum. Pour ce faire, elles vont faire pression et déployer des stratégies pour convaincre le plus grand nombre de personnes physiques de leur vendre les données qu'elles jugeront les plus intéressantes pour elles.

Ainsi, le risque est plus grand de cession imprudente, par un public toujours vulnérable, de ses propres données personnelles. En outre, la mercantilisation des données obligeraient certes les plates-formes à investir beaucoup d'argent pour investir en grand nombre

Toutefois, cela ne veut pas dire que chaque titulaire de données réalise un gain important, tout simplement parce que c'est le grand nombre des données qui représente une valeur marchande considérable et une grande richesse - non pas les données en soi de chaque individu.

La rémunération de l'individu qui céderait ses données ne représenterait pas pour lui – isolément – un bénéfice considérable. De façon indirecte, cette rémunération existe déjà : par le biais de la gratuité d'accès proposée par certains services numériques en échange de la collecte des données La seule différence, c'est que la rémunération ne serait plus en nature, mais en argent ;donc aussi imposable peut-être.

571. Le caractère limité de l'avantage éventuel pour le consommateur, mais également les risques pour lui, désarmé face à de stratégies puissances commerciales (qui ne manqueraient pas de se mettre rapidement en place) expliquent que le Conseil d'Etat français se soit opposé vivement (dans un rapport remarqué intitulé « Le numérique et les droits fondamentaux »[404], paru en 2014) à la voie de la commercialisation de leurs données par les titulaires eux-mêmes.

---

[403] Fabrice ROCHELANDET, *Economie des données personnelles et de la vie privée*, Paris, 2010, La Découverte.

[404] *https://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Etude-annuelle-2014-Le-numerique-et-les-droits-fondamentaux*; Edouard GEFFRAY, « Droits fondamentaux et

Même si, déjà en elles-mêmes, les données ne sont pas totalement étrangères à toute perspective de patrimonialisation, les juristes estiment souvent qu'il leur est toujours associé une dimension éthique et juridique de type particulier. Elles ont beaucoup à voir avec les intérêts moraux des personnes physiques, ainsi qu'avec les libertés fondamentales des personnes physiques, comme les libertés de conscience, d'expression ou d'opinion. Or, de tels intérêts moraux, d'ordre qualitatif peuvent difficilement être correctement évalués en argent. L'exemple allemand[405] pourrait alors s'avérer plus instructif. On pourrait étendre à d'autres pays la solution allemande : à savoir, l'affirmation centrale d'un droit fondamental autour duquel tourneraient l'ensemble des dispositions précises. Il s'agirait d'un droit à l'autodétermination personnelle, qui engloberait l'ensemble des prérogatives des personnes sur leurs données, tout en n'empruntant pas la voie de la patrimonialisation.

572. Bien entendu, l'affirmation d'un tel droit fondamental constituerait une sorte d'axe central susceptible de soutenir des modulations diverses. Il n'exclurait pas toute marchandisation des données, mais poserait des garanties très solides pour éviter vraiment les abus. Nous mesurons donc à nouveau combien le terrain est sensible. On se trouve dans les nuances plus que dans des choix de principe - totalement abrupts, mais inadéquats. En effet, la réalité n'est pas si tranchée.

innovation : quelle régulation à l'ère numérique ? » : *https://www.cairn.info/revue-les-nouveaux-cahiers-du-conseil-constitutionnel-2016-3-page-5.htm*

[405] Droit allemand de la protection des données : *https://www.mittmann-law.de/de_DE/droit-allemand-de-la-protection-des-donnees/*

Section II : Vie personnelle et cadre professionnel.

573. Comme nous l'avons vu précédemment, il semble que le droit se définisse largement comme un point d'équilibre entre des exigences en contraste et en tension. Par exemple, le droit à la protection de la vie privée, d'une part, et celui à l'information ou à l'expression de l'autre. Nous avons envisagé, de façon assez globale, l'espace public. Toutefois, il est un autre espace concerné, plus spécifique. Il présente un effet de caisse de résonance plus fort, car les relations sont plus immédiates, à savoir dans le cadre d'une entreprise.

a. Protection du salarié et vie de l'entreprise

574. Nous n'envisagerons pas tant le respect de points confidentiels au bénéfice de l'entreprise. Comme des secrets internes, dont ne peuvent et ne doivent prendre connaissance, les salariés. Il s'agit de certaines données confidentielles concernant le salarié lui-même, par exemple médicales ou autres.

575. La protection du salarié semble donc être un objectif premier. Dans la mesure où il est en général dans une position de plus grande faiblesse que l'employeur. Cet accent prioritaire relève de ce que l'on pourrait appeler plus largement une forme de discrimination positive. La protection du salarié semble être un objectif prioritaire, notamment pour la Cour Européenne des Droits de l'Homme

Le souci premier d'un employeur est bien entendu que le salarié puisse déployer l'activité la plus efficace ; aussi bien quantitativement que qualitativement. Cela implique, dans une certaine mesure, la surveillance du travail des salariés. Elle peut passer par une surveillance des mails ou des connexions Internet. Cette surveillance est légale mais encadrée. En France par exemple, il y a des règles assez précises. Un principe doit être souligné. Celui de la « vie privée résiduelle ». [406]

Il faut savoir ainsi qu'un employeur peut ainsi vérifier les connexions numériques de ses salariés, et lire éventuellement des documents ou contenus, sauf si ces derniers sont clairement notés confidentiels ou personnels. Bien entendu, les documents confidentiels ne peuvent être lus par l'employeur qu'en présence du salarié et avec son accord. Un arrêt de la Cour de cassation du 2 octobre 2001 précise le périmètre d'utilisation par le salarié de l'outil

[406] Cf. cet excellent article des Echos : *https://www.lesechos.fr/2002/01/courriers-electroniques-y-a-t-il-une-vie-privee-residuelle-sur-le-lieu-de-travail-682905*

informatique de l'entreprise mis à sa disposition pendant son temps de travail pour l'exercice de son activité professionnelle.

576. Ces précisions tentent de concilier la notion de vie privée résiduelle et l'impératif strict qui incombe au salarié de réserver ses outils de travail (non achetés par lui, et qui ne lui appartiennent pas) à des fins professionnelles. Le discernement reste délicat et peut-être en partie arbitraire. Il est à cet égard intéressant de signaler un arrêt de la Cour de cassation en date du 2 octobre 2001 condamnant un employeur pour avoir consulté un fichier portant la mention « personnel ». Toutefois, à rebours pourrait-on dire, la Cour d'appel de Besançon a confirmé, par un arrêt en date du 20 novembre de la même année, un jugement préalablement émis par le Conseil des prud'hommes de Montbéliard. Celui-ci approuvait, en l'occurrence, la sanction prononcée à l'encontre d'une salariée, déléguée du personnel, qui avait adressé plusieurs messages électroniques à une ex-salariée de l'entreprise relatifs à la réorganisation de l'entreprise et à des mutations du personnel, pendant son temps de travail et au moyen du matériel de l'entreprise. Le fond de l'argument de la salariée était l'illicéité de la façon dont sa propre faute professionnelle avait été identifiée. De plus, elle soulignait que la note de service qui interdisait d'utiliser à des fins privées la messagerie n'avait jamais été portée à sa connaissance. Quant à l'entreprise, son argumentation était la suivante : la même salariée avait utilisé le matériel de l'entreprise à des fins personnelles, et ce pendant son temps de travail. Dans son jugement, la cour d'appel de Besançon relève que, si certains messages de la salariée ont un caractère privé, d'autres contiennent des informations sur l'entreprise. Ce qui caractérise autrement les faits incriminés. De plus, il n'est pas prouvé - de façon évidente - que l'employeur aurait usé de moyens illicites pour découvrir la pratique sanctionnée. La Cour se prononce donc en faveur de la légitimité de la sanction. Cette décision s'inscrit dans le droit fil d'autres décisions significatives.

577. Ainsi, par un arrêt du 4 juillet 2000, la Cour d'appel de Rennes a estimé que la faute grave était établie à l'encontre d'une salariée licenciée pour avoir utilisé pendant plusieurs mois la messagerie interne de l'entreprise à des fins personnelles, pour correspondre avec des collègues appartenant au même groupe. La Cour a considéré qu'il n'y avait aucune atteinte au secret des correspondances ;dès lors que l'employeur était en droit de contrôler le bon usage des outils de l'entreprise par les salariés et qu'il n'avait utilisé aucun dispositif de surveillance ou d'interception et qu'aucune manipulation n'avait été démontrée. De même, aucune atteinte au respect de la vie privée n'est commise par l'employeur qui n'a fait que se connecter, comme tout

salarié, à la messagerie électronique pour constater ces excès. Enfin, qui plus est, le règlement intérieur interdisait l'utilisation à des fins privées de l'outil informatique de l'entreprise.

578. Par un arrêt du 25 mai 2001 , la Cour d'appel de Bourges a estimé non caractérisée la faute grave d'un salarié qui avait utilisé à des fins personnelles le matériel mis à sa disposition pour son activité professionnelle. Toutefois, selon la Cour d'appel, le licenciement reposait sur une cause réelle et sérieuse pour avoir utilisé le micro-ordinateur de l'entreprise pour des opérations de Bourse à titre personnel et tenir la comptabilité d'un foyer restaurant dont il assurait la gérance et ce pendant son temps de travail ; ainsi que pour avoir utilisé le téléphone de l'entreprise à des fins personnelles, dans des proportions dépassant les limites du raisonnable.

Cet arrêt est intéressant dans la mesure où la faute grave n'a pas été retenue. En effet, l'employeur avait toléré la présence du salarié pendant un mois après la connaissance des faits. Cela induit donc la nécessité d'agir vite en pareilles circonstances. En tous les cas dans la mesure où l'employeur est en effet dans la possibilité de surveiller l'activité de ses salariés pendant le temps de travail.

579. De même, il est nécessaire que le salarié ait été informé au préalable, en vertu de l'article L. 1222-4 du Code du travail[407],. Tout comme, du reste, le comité d'entreprise conformément à l'article L. 432-2-1[408] du Code du travail de l'existence du système de surveillance du personnel. Il faut rappeler, à cet égard, qu'un salarié qui estime être la victime d'une atteinte à ses libertés fondamentales peut toujours saisir un délégué du personnel. Il est alors possible de mettre en œuvre la procédure d'enquête que prévoit l'article 422-1-1 du Code du travail[409]. Il faut également souligner, toujours dans la perspective de prononcer des jugements équilibrés, que le secret des correspondances, protégé par la Convention européenne des droits de l'homme et l'article 9 du Code civil, demeure une obligation de première importance.

580. L'article L.1121-1 du Code du travail souligne justement que " Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché"

Il faut savoir ainsi que dans l'affaire *Sulzer Orthopédie Cedior,* un salarié a été mis à pied en raison d'une correspondance entretenue avec une ancienne salariée de l'entreprise par messagerie électronique. Malgré le caractère délicat d'une telle correspondance – puisqu'elle

[407] v. legifrance
[408] Abrogé par Ordonnance n°2007-329 du 12 mars 2007 - art. 12 (VD) JORF 13 mars 2007 , Modifié par Loi n°2001-152 du 19 février 2001 - art. 1 () JORF 20 février 2001 legifrance
[409] Modifié par l'art 176 de la loi n°2002-73 du 17 janvier 2002 de modernisation social

était entretenue avec une ancienne salariée de l'entreprise par messagerie électronique - la Cour de cassation a pourtant tenu à insister sur le droit à la vie privée résiduelle dans l'entreprise, en précisant que « le salarié à droit, même au temps et lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique, en particulier, le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçu par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci, même au cas où l'employeur aurait interdit une utilisation non-professionnelle de l'ordinateur ».

C'est pourquoi elle a décidé que la mise à pied disciplinaire n'était pas justifiée. En effet, l'attitude répréhensible de la salariée sanctionnée avec été découverte par l'employeur par le biais d'une consultation irrégulière de l'ordinateur mis à disposition par la société.

581. La législation française du travail est l'héritière d'une longue tradition. Elle est très soucieuse de la protection du travailleur. Certains principes sont fréquemment soulignés. Ainsi, chacun a bel et bien droit au respect de sa vie privée comme le rappelle l'article 9 du Code civil. Certes, il peut y avoir des exceptions. Ce droit peut subir des restrictions, à condition pourtant qu'elles soient nécessaires et proportionnées au but poursuivi (art. L L.1121-1 du code du travail). Dans un domaine qui est celui du flou et du gris, plutôt que du clair et du net, c'est la jurisprudence qui permet de trancher et parfois dans des sens différents.

582. Les droits du salarié, en matière de vie privée, sont limités dans le cadre professionnel. Ils ne doivent pas perturber l'exercice de la profession. Souvent, c'est le bon sens qui est roi en définitive. Toutefois, la balance peut parfois pencher d'un côté ou de l'autre. On pourrait dire une fois de plus : « *In medio stat virtus* ». Par exemple, l'employeur a bel et bien le droit de surveiller ses salariés, mais il faut qu'il soit informé au préalable, et que chacun d'entre eux le soit au préalable à titre individuel (art. L 121-8 du code du travail). Si la vidéosurveillance n'est pas connue, si chacun des intéressés n'a pas été informé à titre personnel, il n'est pas possible de s'en servir contre un salarié même pour le sanctionner suite à une faute bel et bien attestée.

583. À Rouen, en novembre 2013, un employeur a été sanctionné pour avoir porté atteinte à la vie privée d'une salariée qui n'avait pas été prévenue personnellement par écrit qu'une caméra était dirigée vers son poste de travail (CA de Rouen du 5.11.13, n° 3/00599). En effet, la surveillance des salariés n'a rien à voir avec des dispositifs que l'on peut mettre en place pour se protéger des attaques extérieures et des risques d'intrusion.

584. Pour mettre en place un dispositif de surveillance destiné à conjurer les risques d'intrusion, il n'est pas nécessaire de prévenir les salariés. En revanche, il n'est évidemment pas possible de servir de tels dispositifs dans les cas où ils livreraient aussi la preuve d'une faute professionnelle d'un employé ; sauf si celui-ci avait été au préalable dûment informé qu'une tel dispositif pouvait avoir une finalité seconde à celle d'une surveillance tournée vers l'extérieur. De même, l'employeur ne peut pas installer un système de géolocalisation sur le véhicule de fonction de son salarié sans l'en informer. Même si un tel système est installé, le salarié doit pouvoir le désactiver lorsqu'il utilise le même véhicule dans le cadre de sa vie privée (CA de Bordeaux du 25.11.08, n° 07/05964). Tout usage de semblables dispositifs, à des fins qui n'ont pas été prévues et annoncées au départ serait illégal, surtout si c'est au détriment du salarié, sont prohibés.

b. Un bon équilibre à trouver

585. Un employeur peut consulter l'ordinateur d'un salarié et ouvrir l'armoire de son bureau, consulter aussi des documents sauf si ce dernier a mentionné - de façon explicite - qu'ils étaient de nature privée.

Bien entendu, une correspondance d'ordre privée ne peut pas être utilisée contre le salarié. Tout ce qui est - en soi - d'ordre privé demeure à protéger. Cependant, en l'absence d'une mention explicite le spécifiant, les documents d'un employé sur son lieu de travail sont présumés relever de son activité professionnelle et non de sa vie privée. Il ne suffit pas que des courriels et fichiers se trouvent dans le disque dur d'un ordinateur émanant de la messagerie électronique personnelle du salarié pour qu'ils soient considérés comme privés.

586. Concrètement, il va de soi que la seule appellation «mes documents» ne suffit pas à attribuer à un fichier un caractère personnel (cass. soc. du 10.5.12, n° 11-13884). Des échanges de nature privée, comme un mail dans lequel un salarié se plaindrait à sa petite amie de la façon dont il est traité par son patron, ne peuvent être utilisés contre le salarié. A l'inverse, par exemple, un mail - même confidentiel - adressé à un autre salarié de l'entreprise (cass. soc. du 2.2.11, n° 09-72450), le peut.

587. Le principe de base demeure. Le salarié n'a pas à utiliser son ordinateur, ou son lieu de travail, pour ce qui relève de sa vie privée. Ainsi, il n'a pas le droit de surfer sur l'Internet comme il le souhaite. L'utilisation abusive de l'Internet peut constituer une cause de licenciement. En principe, le salarié doit uniquement se connecter sur l'Internet pour des raisons professionnelles.

588. Ces principes valent également, même s'ils ne sont pas explicitement rappelés par le règlement intérieur. En effet, ils sont considérés comme allant de soi dans le cadre de la vie professionnelle. On peut, cependant, présumer que, pour établir une utilisation abusive, sauf mention explicite très précise, il est nécessaire que le nombre de connexion soit conséquent et répété. Comme dans le cas d'une salarié qui avait effectué plus de 10 000 connexions en seulement deux semaines, sur des sites n'ayant aucun rapport avec son travail (tourisme, marques de prêt-à-porter, sorties, réseaux sociaux - Cass. soc. du 26.2.13, n° 11-27372).

589. Le seul fait d'un usage ponctuel, pour de possibles raisons impératives, ne saurait cependant constituer une faute grave et justifier un licenciement. La justice a ainsi refusé de valider le licenciement d'une assistante fondé sur un usage privé de l'Internet (mais sans précision de durée) et du téléphone (CA de Douai du 31.5.13, n° 12/02753).

590. À nouveau, la réflexion juridique laisse se dégager le sentiment d'une difficulté à trancher de façon trop générale, en raison d'une tension entre d'exigences contradictoires. Le rôle de la jurisprudence paraît plus que jamais important.

TITRE II : LE CONTROLE D'UNE NOUVELLE CRIMINALITE (Droit pénal et droit international)

Chapitre I : L'émergence de la cybercriminalité

591. Comme nous l'avons déjà souligné, les grands défis du numérique concernent différentes branches du droit. Ce qui lui impose d'opérer une sorte de synthèse harmonieuse de ces différents instruments.

Dans une période de mutation globale de la société, par exemple celle récente sur le coronavirus, la criminalité prend des formes nouvelles, dopée d'ailleurs par les développements technologiques. Des parades sont recherchées et parfois trouvées. Au fur et mesure, la criminalité, décidément très industrieuse, trouve d'autres stratégies. On assiste à une sorte d'enchaînement : le développement de la criminalité suscite, en réponse, le développement des mesures de prévention, et réciproquement.

592. Nul ne peut prévoir les formes futures que prendra la cybercriminalité ni son étendue. Ce qui suscite bien entendu une forte inquiétude. Les nouveaux défis qui se posent justifient que l'on accorde une attention particulière à la question. On ne peut ignorer l'inquiétude qui monte et parfois aussi un phénomène de panique[410].

Les médias attisent cette panique, dans un but intéressé, ou de façon presque automatique. Le raffinement des menaces, ainsi que la nécessité de trouver des parades très élaborées doivent nous inciter à solliciter davantage les experts, tout en contrôlant leur travail au travers de politiques publiques structurées. L'expertise est une chose ; la décision politique en est une autre. La question de la place des experts revêt une très grande importance[411].

593. On peut se demander dans quelle mesure il est pertinent et démocratique de garder une telle différence entre les experts supposés compétents et la société civile. Celle-ci entend, elle aussi, réagir face aux risques. Notamment au travers de la constitution d'association et sans attendre les décisions du sommet politique (de l'exécutif), ni d'experts qui ont un savoir mais n'ont pas pour autant une sorte de super-légitimité démocratique[412].

594. Une clarification en la matière redonnerait en même temps toute sa spécificité à la contribution que peuvent apporter en propre les experts, sans arrogance technocratique, mais avec une vraie

[410] David GARLAND, « On the concept of moral panic », 2008. *https://journals.sagepub.com/doi/10.1177/1741659007087270*
[411] Steven BRINT*, In an Age of Experts. The changing Roles of Professionals in Politics and Public Life*, Riverside, UCRiverside, 1996. Un ouvrage déjà classique mais qui pose beaucoup de bases.
[412] Michel CALLON, Pierre LASCOUMES, Yannick BARTHE*, Agir dans un monde incertain. Essai sur la démocratie technique,* Paris, Le Seuil, 2001.

compétence[413]. D'une certaine façon, nous assistons à l'émergence d'un monde de l'insécurité, où une sorte de cohésion globale d'ensemble[414] prend forme non pas à partir d'un élément positif mais en tant que les menaces deviennent globales, climatiques, sanitaires, terroristes, et ensuite économiques. Il semble aussi que nous soyons désormais entrés dans un monde où le risque est constant. La perspective ne sera plus tellement de l'éviter complètement, mais de l'encadrer. De le contrôler autant que possible et par là de le limiter.

595. Par conséquent, un monde instable devient la norme. Il ne s'agit donc plus d'en sortir enfin mais de construire dans ce monde-là et avec lui. Ce qui est évidemment une perspective moins rassurante et moins euphorique. Il s'agit en revanche d'un défi redoutable et exigeant. Le réalisme est peut-être l'une des premières qualités du juriste.

Section I : Visages divers d'un risque croissant.

a. Le retour du risque

596. La question de la gestion des risques semble devoir devenir prioritaire[415]. Cela implique, d'un point de vue statistique et prospectif, l'évaluation des risques à venir, singulièrement délicate.

Des choix individuels comme des décisions collectives, des stratégies privées comme les politiques publiques doivent en tout cas tenir compte d'une estimation et des sélections des risques. Lesquels d'entre eux sont-ils incontournables ? Comment faire alors pour les limiter et s'habituer à leur présence ? Lesquels au contraire sont-ils évitables et à conjurer ? Comment tenir compte du clivage qui peut exister, dans des sens différents d'ailleurs, entre l'évaluation faite par des experts ou les puissances et celle que se fait à lui-même chaque individu, parfois de façon très instinctive. Comment envisager d'éventuels arbitrages ? Faut-il privilégier la sécurité quitte pour cela à paralyser certaines initiatives ou la vie économiques ? Ou, au contraire, vaut-il mieux accepter certains risques pour obtenir des satisfactions plus grandes ou davantage de croissance ?

597. Il semble clair que ce genre de questions ne se posent pas simplement dans le champ de la criminalité, mais face à tous les risques possibles, qui surgissent, resurgissent. Dans le cas d'une

[413] Philippe ROQUEPLO, *Entre savoir et décision, l'expertise scientifique,* Paris, INRA, 1997.
[414] Didier BIGO, « La mondialisation de l'(in)sécurité ?Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation » in *Cultures et Conflits*, 2005, 53-101.
[415] Claude GILBERT, « la fabrique des risques » in *Cahiers internationaux de sociologie,* 2003/1, 114, 55 -72.

pandémie, de telles questions ne manquent pas non plus de se poser. Comme en témoigne l'actualité récente du Covid-19. Pour reprendre des péripéties encore toute fraîches : Faut-il imposer un confinement strict très désagréable et avec un impact redoutable sur l'économie, pour limiter un risque ? Ou, au contraire, ne vaudrait-il pas mieux assumer en partie un risque ? Car vouloir le conjurer de façon entraînerait par ailleurs des dommages collatéraux trop importants.

598. On le voit, le questionnement qui surgit face à la menace que fait peser la cybercriminalité est un grande partie semblable à celui qui ne manque pas de s'imposer quel que soit le risque. On ne peut donc aborder de façon cloisonnée la question de la cybercriminalité, sans la relier à une sorte de méta-problématique, si l'on ose dire. Celle-ci serait celle des options possibles face à un risque, souvent diversement évalué du reste.

En effet, tant qu'il n'est pas devenu réalité, il est difficile de cerner l'extension exacte du mal qui adviendra. Dans un monde chaotique comme celui qui nous entoure, pour surmonter une réaction purement émotionnelle, il semble important d'appréhender les risques sous tous leurs aspects réels et virtuels. Ceci, afin de redéfinir de grandes orientations - évidemment modulables ensuite - selon les grandes options des individus et des institutions.

599. Rien de tout cela n'est facile. Toutefois, pour quelque risque que ce soit, il semble urgent et prioritaire, en amont, de définir le cadre dans lequel le risque sera traité par les différents acteurs. Ceci, sachant qu'un risque peut justement être aggravé par une attitude malheureuse, inappropriée face à lui.

C'est cette gestion globale des risques qui semble donc devoir focaliser de façon prioritaire et privilégiée notre attention, aujourd'hui[416]. Cela suppose aussi, dans une perspective initiale, et très théorique, de déterminer quels sont les principes qui doivent orienter les grands choix (sur lesquels tout le monde n'est pas forcément d'accord, comme le principe de précaution[417]).

600. L'un des problèmes les plus délicats, les plus complexes et les plus ambivalents à gérer est celui des médias qui peuvent, en effet, par les informations transmises, éveiller et entretenir une

[416] Patrick LAGADEC*, La civilisation du risque*, Paris, Seuil, 1981 *; Apprendre à gérer les crises*, Paris, éditions d'Organisation, 1993 ; *Traité des nouveaux risques*, Paris, Folio, Gallimard, 2002 ; *La Fin du risque zéro*, Paris, Eyrolles-Société, 2002. ; *Apprendre à gérer les crises,* Paris, Éditions d'Organisation, 1993.

[417] René AMALBERTI et Claude GILBERT, *De la gestion des risques technologiques à la gestion des dangers collectifs,* Paris, *Encyclopaedia Universalis*, Paris, 2001, p. 90-96. Philippe KOURILSKY et Geneviève VINEY, Le principe de précaution. Rapport au premier ministre, Paris, Odile Jacob, 2000.

conscience citoyenne ; mais qui peuvent aussi contribuer par une désinformation avec de trop fortes résonances émotionnelles. Cette attitude mène à des raccourcis - hélas - suggestifs, à brouiller les pistes, embrumer les esprits, susciter la panique, ou, au contraire, minimiser des risques réels, cacher ce qui ne va pas.

Les chaînes d'information peuvent, par un manque de précision et de rigueur, susciter une peur globale, sans mettre en garde - de façon ciblée - contre ce qui est véritablement dangereux.

601. Un peu comme la célèbre langue d'Esope, les médias sont souvent la meilleur et la pire des choses. Pour illustrer sans doute cet impact des médias, mais aussi pour se lancer comme jeune journaliste de 23 ans, Orson Welles - on s'en souvient - a semé la panique dans une bonne partie des Etats Unis, le 30 octobre 1938, en suggérant une invasion de l'Amérique par des Martiens. Le problème de l'impact des médias et en particulier de l'impact négatif doit absolument être souligné[418].

Cela ne veut évidemment pas dire que le remède passe obligatoirement par la censure. On peut imaginer plutôt la promotion concurrentielle d'une information de qualité. Ce problème du rôle, éventuellement néfaste, mais aussi positif des médias ne peut être éludé. Dans un tel contexte, le plus important n'est pas de faire face par un attitude volontariste, mais de reconstruire une sorte de résilience continue ; en gardant une attitude continue de vigilance et en se préparant à une gestion régulière de la sécurité.

602. Il ne faut pas s'épuiser à vouloir colmater toutes les brèches, ou à pourchasser chaque délinquant. Ce qui est un combat vain, à l'image de celui d'un Don Quichotte, le célèbre personnage de Cervantès, s'en prenant aux moulins à vent. Ainsi, la cybercriminalité prend aujourd'hui une place croissante dans la société, grâce à l'accessibilité de l'iInternet et à la globalisation des échanges.

603. Nous ne sommes donc plus en face d'actes isolés, mais à un phénomène d'ensemble. À savoir, un risque majeur en matière de sécurité ; face auquel toute la société est confrontée. Il induit une stratégie globale de défense et de résistance[419]. Elle doit susciter une nouvelle forme d'expertise, avec beaucoup d'esprit critique et de vigilance. Ce qui exige des études en amont et en aval : une véritable perspective stratégique. En effet, il s'agit à la fois de guérir et surtout de prévenir…ce qui pourtant demeure largement imprévisible.

---

[418] Cyril LEMIEUX, *Mauvaise presse. Une sociologie compréhensive du travail journalistique et de ses critiques,* Paris, Métailié, 2000.

[419] Franck GUARNIERI et Eric PRZYSWA, « Cybercriminalité et expertise. : enjeux et défis » in Sécurité et stratégie, 2012, 4, 49-55.

b. Cybercriminalité et contrefaçon

604. Pour aborder ce phénomène croissant et inquiétant de la cybercriminalité, bien qu'insuffisant, il est - de prime abord - heuristiquement fécond, de s'appuyer sur le phénomène de la contrefaçon. Ce dernier constitue un délit ; ou plutôt un ensemble de conduites délictueuses à rapprocher, du reste, d'autres qui lui sont voisines[420]. La contrefaçon est la reproduction ou l'imitation d'un objet qui usurpe des marques de produits dans un but lucratif bien entendu, et donc quelque chose d'illégal aussi bien dans les moyens déployés que dans les fins.

605. Il s'agit d'une tromperie. Elle touche de très nombreux secteurs : allant des œuvres artistiques aux produits de luxe, en passant par les médicaments, ou les vêtements. On trouve même aujourd'hui des minéraux ou des fossiles contrefaits. Bien entendu, l'une des formes de contrefaçon les plus anciennes et aussi les répandues, les plus traquées et sévèrement punies, est celle de la monnaie[421].

606. La contrefaçon façonne et alimente aujourd'hui un marché très lucratif et à vaste échelle[422], réunissant des enjeux considérables. De sorte qu'il y aussi une volonté et une nécessité de guerre à la contrefaçon[423]. La contrefaçon ne s'exerce pas toujours au détriment d'un acheteur éventuel (qui y voit une " bonne affaire "). La mondialisation augmente les échanges, ce qui augmente aussi, en cascade, la contrefaçon. D'autant plus que les systèmes régulateurs sont pris en défaut et moins performant dans le cadre d'une explosion d'activités économiques. Certains pays producteurs comme la Chine, la Turquie, l'Inde ou la Russie et les pays de l'Europe de l'Est sont des champions de la contrefaçon des biens ; à laquelle s'ajoute, de plus en plus semble-t-il, la contrefaçon de documents d'identité.

Il y a dans la contrefaçon quelque chose de l'ordre du parasitisme[424] : une atteinte à la propriété, y compris intellectuelle. Bien entendu, la contrefaçon ne se déploît pas seulement par pur plaisir ludique de la transgression, mais pour des raisons d'intérêts. Ce qu'il y a de plus objectif.

---

[420] Gérard BEAUR (dir.), Hubert BONIN (dir.) et Claire LEMERCIER (dir.), *Fraude, contrefaçon, contrebande de l'Antiquité à nos jours*, Paris, Droz, coll. « Publications d'histoire économique et sociale internationale », 2017.
[421] Gildas SALAUN, « La fausse monnaie et sa répression à la fin du Moyen Âge », in *Monnaie magazine*, mars 2020, p. 50-55.
[422] Pierre DELVAL, *Le marché mondial du faux*, Paris, CNRS, 2010.
[423] Bleuzenn MONOT*, La guerre de la contrefaçon*, Paris, Ellipses, 2009
[424] Godefrroy de MONCUIT, « Les relations entre contrefaçon et parasitisme » in *Le Concurrentialiste*, 2 mai 2014.

607. C’est surtout le développement technologique qui permet une contrefaçon rapide et aisée de certains produits comme Le cadre légal est également très variable, très disparate. Ce qui permet de se faufiler entre les différents pays. Le moteur de la contrefaçon est souvent le désir d’obtenir des devises fortes, comme le dollar ou l’euro : c’est-à-dire, la monnaie d’un pays qui a une activité économique importante.

Plus il est facile de transporter rapidement des objets produits, plus il y a de contrefaçon. Cela est singulièrement vrai de biens dématérialisés, comme ceux de la révolution numérique. Il nous faudra revenir sur cette remarque importante.

608. Dans le monde actuel, il est coûteux de vérifier l’origine des produits. De même, la circulation des capitaux n’a jamais été aussi fluide. La barrière des langues et de mauvaises traductions permettent souvent de faire passer la contrefaçon. La contrefaçon permet également, souvent, d’échapper à des taxes. Le caractère illégal - donc discret - de la contrefaçon rend difficile l’estimation de son importance.

609. Les États luttent en général, mais de façon inégale et différenciée. La contrefaçon est considérée, en France, par exemple, comme une fraude grave, punissable d’amendes et de saisies. Il peut s’agir d’un délit et non d’une simple infraction, dans le cas de grands trafics la contre-façon peut valoir un emprisonnement de trois ans au plus.

610. Depuis juin 2016, il peut y avoir une circonstance aggravante, dans le cas de l’existence d’une ou de plusieurs bandes organisées, avec des peines bien plus lourdes. Il est important de noter que l'article L335-3 du Code de la propriété intellectuelle souligne que, “relève aussi du délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi”.

Pour utilisation d’une œuvre, il faut, sauf exception, et sauf usage dans un cadre privé et familial, l’accord explicite de l’auteur ou des ayant-droit.

c. La pandémie de la cybercriminalité

611. L’étude systématique de la contrefaçon, aussi bien d’un point de vue strictement juridique que sociologique, peut ainsi nous permettre de mieux comprendre le phénomène de la cybercriminalité. En effet, il y a une sorte d’analogie entre les deux. Toutefois, il faut prendre

conscience de l'ampleur considérable de la cybercriminalité qui fait d'elle l'un des phénomènes les plus inquiétants.

612. Cette urgence a été un peu perdue de vue ces derniers mois, peut-être en raison de l'épidémie du Covid-19. Alors que l'on pensait, sans doute à tort, être parvenus à la fin des épidémies de grande ampleur en Europe. Alors que les savants[425], ou même un auteur de roman policier comme Fred Vargas[426] nous mettait en garde. Occidentale. La dernière la plus meurtrière ayant été la grippe espagnole, après la Première Guerre Mondiale[427].

La menace de graves problèmes induits par la cybercriminalité a retenti dans le contexte d'un ciel serein, en partie tout au moins (ou du moins dans le cadre d'une minimisation de risques graves venant de la nature). Et ce, malgré des livres ou des films, qui par l'outrance même de la peur qu'ils pourraient susciter, nous ont peut-être détournés, parfois, de l'attention à la survenue d'une crise sanitaire.

613. Au cœur de cette crise, l'Internet a bien résisté et a permis à beaucoup de rendre cette crise et en particulier le confinement moins insupportables ; tant d'un point de vue psychologique qu'économique, avec le développement du télétravail[428].

614. Il y a encore quelques mois, le télétravail peinait à avancer dans certains pays comme la France. Le confinement lui a non seulement octroyé une nouvelle légitimité, mais encore lui a permis de faire ses preuves : il est réalisable à large échelle et efficace. Cela ne veut cependant pas dire qu'il constitue une sorte de « panacée » à aucun point.

Bien entendu, de façon paradoxale, la crise du covid-19 a également montré combien le présentiel était important.

615. La crainte d'une saturation des réseaux en France ne s'est pas vérifiée. Peut-être parce que la perspective des jeux olympiques a conduit la France a maximaliser d'ores et déjà ses potentialités. En tous les cas, la crise sanitaire a conduit à un plus grand recours au numérique. Ce dernier, est donc présenté comme un bienfait et une chance. Dont on mesure cependant aussi

[425] Dès les années 1930, les plus célèbres divulgateurs en épidémiologie Charles Nicolle s'exprimait en ces termes : « Il y aura donc des maladies nouvelles. C'est un fait fatal. Un autre fait, aussi fatal, est que nous ne saurons jamais les dépister dès leur origine » (Charles NICOLLE*, Destin des maladies infectieuses*, Paris, Presses Universitaires de France, 1939).

[426] Par exemple dans un roman. Cf. Fred VARGAS*, Pars vite et reviens tard*, Paris, Viviane Hamy, 2001.

[427] Freddy VINET, *La Grande grippe. 1918, la pire épidémie du siècle*, Paris, Vendémiaire, 2018.

[428] Raymond-Marin LEMESLE et Jean-Claude MAROT, *Le télétravail,* Paris, Presses Universitaires de France, Que sais-je ? »,(no 2809), 1994.

les limites face à la vie « réelle ». Une vie « réelle » qui demeure à bien des égards irremplaçables.

616. Certains ont peut-être été forcés de surmonter leur peur et de s'y mettre. Tout cela est positif, mais une certaine euphorie ne peut certainement pas nous aveugler sur le risque énorme de la cybercriminalité. Ce dernier, fut un peu moins présent à nos esprits pendant la crise sanitaire. Telle une épée de Damoclès, il reste de plus en plus lourd et menaçant.

La civilisation de la surinformation focalise notre attention sur un risque, peut-être aux dépens des autres. On peut supposer que l'obsession des esprits au sujet d'un risque ne soit voulue ou entretenue (pour réel que soit le risque, ou qu'il soit entretenu), pour faire passer d'autres pilules ; faire oublier d'autres risques.

617. D'une certaine façon, la menace d'un virus comme le Covid-19 peut nous rendre plus attentifs à une attaque informatique. En effet, il y a quelque chose de commun entre les deux types de virus[429]. Un virus informatique, tout comme un virus biologique, se propage en utilisant les facultés de l'hôte. Pour comprendre l'apparition historique des virus informatiques, il faut se souvenir que les premiers programmes autonomes conçus dans une perspective ludique. Il ne semblait pas possible que l'on puisse un jour y avoir des conséquences sérieuses sur la vie sociale, la marche des peuples et la cohérence des sociétés. Les tout premiers logiciels de ce type se présentaient comme des outils à la fois plaisants et sophistiqués de divertissement. Par exemple, en 1970, trois informaticiens de talent, Victor A. Vissostsky, Robert Morris et Douglas McIlroy, inventent Core War. Chaque joueur écrit un programme et le charge en mémoire vive. Par la suite, un ingénieux système d'exploitation, très novateur pour l'époque, adroitement multitâche, exécute successivement chacun de ses programmes. La perspective est ludique. Elle prône le divertissement. Nullement politique ou guerrière. Ni lucrative, et encore moins associée à la délinquance ou à la criminalité.

618. Cette première observation nous semble importante, aussi bien pour le sociologue que pour le juriste. En effet, de l'anodin ou du plaisant peut dériver du dangereux. Cela veut dire que la vigilance doit toujours être de mise, y compris lorsqu'a priori personne n'envisage un risque ou une conduite agressive et délictueuse. Au départ, mais dans un cadre inoffensif et ludique, il

[429] D'où le choix terminologique et le parallèle établi. Cf. Mark Allen LUDWIG, *Naissance d'un virus : Technologie et principes fondamentaux*, Paris, Bordas, 1993 ; *Mutation d'un virus : vie artificielle et évolution*, Paris, Addison-Wesley France, 1996 ; *Du virus à l'antivirus : guide d'analyse*, Paris, Dunod, 1997. Aussi Éric FILIOL, *Les Virus informatiques : théorie, pratique et applications*, Paris, Dunod, 2009. Le premier à utiliser le terme de virus en infoprmatiquie aurait été Leonard Adleman, à la fois informaticien et spécialiste en biologie moléculaire.

s’agit ni plus ni moins de détruire les programmes adverses, tout en assurant sa propre prolifération et son essor. Les programmes sont habilement conçus. Ils sont capables de se recopier, de se réparer, de se déplacer en différentes zones de la mémoire et « d'attaquer » les programmes adverses. Il n’y a donc pas tellement, dans ce jeu, un gagnant que des perdants. Un peu comme dans le célèbre jeu télévisé « le maillon faible », où les candidats sont cruellement éliminés au fur et à mesure. Un perdant est celui qui voit tous ses programmes inactifs ou détruits. Le vainqueur est en fait un survivant, qui possède le plus grand nombre de copies actives dans le jeu. On peut dire que ce jeu est à l’origine des virus, mais sans avoir la même intention « sérieuse ». Une dizaine d’années plus tard, le magazine « Scientific American » lance quant à lui un jeu informatique qui consiste à concevoir de petits programmes qui entrent en lutte et se dupliquent, s’efforçant d’infliger à l’autre des dégâts.

619. Les virus informatiques d’aujourd’hui n’en sont pas loin. Deux ans plus tard, l'ARPANET qui précède l’Internet est infecté par *Brain*, virus renommant toutes les disquettes de démarrage de système en *(C)Brain*. Les créateurs de ce virus y donnaient leurs nom, adresse et numéro de téléphone, car c'était une publicité pour eux. Nous ne sommes donc pas encore dans la criminalité clandestine. Il s’agit plutôt d’une provocation et d’une preuve du caractère rapide et fructueux de la recherche. Un peu cultivée pour elle-même et par plaisir et non dans un but coupable.

620. Comme chacun sait, depuis, les virus se sont diversifiés et perfectionnés. Le virus classique est un morceau de programme, souvent écrit en assembleur, qui s'intègre dans un programme normal, quelquefois à la fin. Ainsi, chaque fois que l'utilisateur exécute ce programme « infecté », il active le virus, lui redonne vie et efficacité. Ce méchant parasite en profite alors pour s’immiscer dans d'autres programmes exécutables et les perturber. En outre, il peut, après un certain temps (éventuellement assez long) ou un événement particulier qui le déclenche, exécuter une action prédéterminée.

621. Cette action peut aller d'un simple message anodin, à la détérioration de certaines fonctions du système d'exploitation, ou à la détérioration de certains fichiers ; ou même encore, au pire, la destruction complète de toutes les données de l'ordinateur. On parle dans ce cas de « bombe logique » et de « charge utile ». Ce dernier adjectif qualificatif n’étant peut-être pas judicieusement choisi.

622. Un virus de *boot*, quant à lui, s'installe dans un des secteurs de *boot* d'un périphérique de démarrage, comme un disque dur, mais sans modifier un programme, comme un virus normal.Il remplace un programme de démarrage existant. Il agit un peu comme un virus « *prepender* »

(qui s'insère au début). Toutefois, le fait d'infecter aussi un périphérique vierge de tout logiciel de démarrage le distingue du virus classique ; qui ne s'attaque jamais à « rien ».

623. Il faudrait accorder une attention toute particulière aux macros de logiciels de la suite *Microsoft Office*, qui s'active chaque fois que l'utilisateur met en œuvre le logiciel. En 2003, sont apparus les virus-vers. On les nomme ainsi, car leur mode de propagation est lié au réseau, comme des vers, en général via l'exploitation de failles de sécurité. En outre, leur action est discrète et ne conduit pas à la destruction de l'hôte ; pas plus que les vers ne tuent ceux qui les portent en eux (en général). Toujours à l'instar des vers, ils poursuivent des buts à visée large, tels que l'attaque par saturation des ressources ou attaque *DoS* (*Denial of Service*) d'un serveur par des milliers de machines infectées qui se connectent en même temps.

624. Il y a encore les virus de type *batch*, apparu à l'époque où *MS-DOS* était le système d'exploitation en vogue. Ce sont des virus « primitifs ». Sans doute, ils sont eux aussi capables de se reproduire et d'infecter d'autres fichiers, mais ils sont lents et ont un pouvoir infectant très faible, de sorte que leur dangerosité n'est pas si grande.

625. L'ensemble de ces virus présente un certain nombre de caractéristiques communes, comme par exemple le chiffrement, le polymorphisme, le métamorphisme et la furtivité. Ce sont des termes techniques mais qui désignent des réalités assez simples. À chaque réplication, le virus est chiffré (de même que l'on parle d'un code diplomatique pour échanges secrètement des informations entre états). Cela veut dire que les instructions y sont dissimulées derrière le chiffre. Tout simplement pour que l'on ne puisse voir la présence de ce virus ou d'un code suspect.

626. Les types de chiffrement ou de dissimulation peuvent varier, du plus simple au plus subtil. Néanmoins, ce qu'il y a de commun à chaque fois, c'est le caractère sournois et déloyal du virus qui avance invisiblement , si l'on ose jouer sur les mots.

Pour les combattre, on a mis sur pied un certain nombre de logiciels antivirus - plus ou moins efficaces et puissants, destinés en principe à détecter des virus, à les détruire, à les isoler, mais aussi quelquefois à réparer les fichiers. Bien entendu, ces antivirus utilisent des moyens très diversifiés et perfectionnés. Dans le détail desquels nous ne pouvons entrer ici : comme la reconnaissance de séquences d'octets caractéristiques (signatures) d'un virus particulier, la détection d'instructions suspectes dans le code d'un programme, la création de listes de

renseignements sur tous les fichiers du système ou encore la surveillance des lecteurs de support amovible.

627. Comme pour les virus biologiques, en informatique ce sont les systèmes et logiciels les plus répandus qui sont les plus atteints (en contact avec les autres). Dans la mesure où l'accès à l'Internet est de plus en plus banalisé sinon généralisé, c'est un plus grand nombre de personnes qui est touché. L'infection par des virus informatiques devient un phénomène de masse. De même que les virus biologiques sont favorisés par la circulation de la population et la promiscuité. La contamination se fait de plus en plus rapidement, et de plus en plus facilement. Les virus s'approprient, par exemple, sans grande difficulté, des adresses de courriel présentes sur la machine infectée. Ce qui contribue à leur diffusion très rapide et très large. Enfin, l'interconnexion des ordinateurs en réseaux locaux favorise encore, et considérablement, la propagation des virus trop heureux de trouver de nouvelles cibles potentielles. Il est à noter que les virus peuvent également toucher la téléphonie mobile aujourd'hui. Le premier virus qui s'attaqua à elle remonte à 2004. Le risque est semble-t-il moins élevé que pour les ordinateurs. Néanmoins, le fait n'est pas anodin. Notamment, si l'on tient compte du grand nombre de personnes qui utilisent la téléphonie mobile, dans la jeune génération en particulier.

628. L'image que nous donne un virus naturel est celle d'un monde en perpétuel mutation, où l'inattendu se présente de plus à plus à nous, plus vite que prévu aussi. Chaque fois que l'on crée une arme défensive, comme un vaccin par exemple, la nature en crée une nouvelle[430]. Il est donc singulièrement bien inspiré de parler de virus aussi pour le numérique. De filer ainsi la métaphore pour la permanence, la mutation constante et l'imprévisibilité d'une menace.

d. ***Les nouveaux visages de la délinqu*ance[431]**

629. Par conséquent, la cybercriminalité ne cesse de se développer considérablement dans le monde actuel. Ce qui sème l'inquiétude, sous une forme sourde ou parfois de panique chez les internautes. Les criminels utilisent les données personnelles des uns et des autres, personnes physiques ou morales, dans l'intention de commettre des crimes et des délits d'une étendue et d'une gravité encore difficiles à évaluer.

[430] Frédéric KECK, *Les sentinelles des épidémies*, Bruxelles, Zones sensibles, 2020.
[431] Éric FREYSSINET*, La cybercriminalité en mouvement*, Cachan, Hermes Science Publications, coll. « Management et informatique », 2012.

De même, il existe un *dark web*, sur lequel il est hélas possible d'acheter et de vendre des produits et des services illégaux : dont, par exemple, des drogues, des armes, de la pornographie infantile, ou même des tueurs. Les secrets les plus confidentiels des gouvernements sont même menacés.

630. La cybercriminalité atteint désormais un niveau record, montant désormais à des milliard et des milliards de dollars. L'ampleur du phénomène présente quelque chose de vertigineux. L'Internet offre aux criminels des possibilités d'agir inconnues jusqu'alors. La cybercriminalité désigne les crimes et délits effectués en lien avec l'Internet, un ordinateur ou un portable.

Ces deux derniers peuvent être la cible d'une attaque, mais également être utilisés pour attaquer. Un cybercriminel peut accéder aux informations personnelles d'un utilisateur, à des informations confidentielles professionnelles, à des informations gouvernementales, ou pour désactiver un appareil. La cybercriminalité est aussi une façon nouvelle et dangereuse de s'approprier l'espace commercial[432], difficile à contrôler et faisant peser de très lourdes menaces.

631. Dans une première approche de la cybercriminalité, moins affinée d'un point de vue juridique, mais mettant en relief la variété des possibles, on peut distinguer différents types de nuisances. D'abord, en plus conventionnel, il faut signaler les attaques visant à profiter de la crédulité (du manque de vigilance, de l'ignorance ou de la peur) dans le but de soustraire, en général à des particuliers, des informations confidentielles, à des fins non légales ; souvent avec de graves conséquences.

On peut faire ensuite mention d'autres graves infractions, comme des extorsions de fonds, de la fraude liée à la carte de crédit, de la fraude commerciale, des abus de confiance et diverses escroqueries parfois très inventives, des menaces exercées (par exemple de vengeance), des usurpations d'identités ou des détournements de mineurs. On le voit, il s'agit dans beaucoup de cas de crimes et délits traditionnels, mais qui sont en quelque sorte surdimensionnés par les apports des nouvelles technologies, rendus plus aisés à commettre et parfois plus grave aussi.

À cela, s'ajoutent des attaques plus directement technologiques, qui exploitent les failles toujours possibles, et restées parfois inaperçues pendant longtemps, de l'outil informatique. Les plus répandues sont les suivantes : l'installation de programmes-espions ou de programmes-

[432] Stephane LEMAN-LANGLOIS, « Questions au sujet de la cybercriminalité. Le crime comme moyen de contrôle du cyberespace commercial », in *Criminologie,* 2006, 39, 1, 63-81.

pirates, diverses détériorations, le vol d'informations parfois même classifiées, dans des buts divers (qui peuvent également être très graves, à savoir terroristes).

632. On distingue souvent des attaques de type purement opportuniste. Elles visent à atteindre un grand nombre de victimes possibles, comme la création ou l'achat d'un logiciel malveillant. Ce dernier, permettant de s'emparer, parfois de façon définitive et totale, des appareils des victimes.

Il faut également identifier la création de sites infectés et pervers, et l'infection de sites existants. Quelquefois les attaques sont véritablement ciblées, très précises et très bien ajustées. Dans ce cas, une telle attaque a de grandes chances de réussir ; de provoquer de graves conséquences. Elle passe - en général - par plusieurs étapes soigneusement mises en place. D'abord une récolte d'informations. Ce qui est un préliminaire obligé. Ensuite, un balayage du réseau. Il consiste à tester les systèmes cibles, afin de relever les failles, y compris les possibles failles humaines qui relèvent de ce que l'on appelle quelquefois l'ingénierie sociale.

633. Il convient de relever - en particulier - le danger du fichier piégé. Il s'agit d'un courrier contenant un « Cheval de Troie », qui vise à prendre le contrôle à distance d'une machine une fois que la victime l'aura activé. L'expression très suggestive de « Cheval de Troie », nous renvoie donc à un épisode célèbre de l'*Iliade*. Cette grande œuvre poétique prêtée à Homère.

Suivant le conseil du rusé Ulysse, des guerriers grecs se cachent à l'intérieur d'un magnifique cheval, afin de pouvoir pénétrer dans la ville de Troie. Ils font mine de l'offrir en cadeau, pour que les Troyens veuillent bien le laisser entrer. Avec succès. Les guerriers sortent ensuite du cheval et massacre les Troyens. De même, certains virus procèdent de façon particulièrement insidieuse. En apparence inoffensif et bienveillant, le cheval de Troie informatique contient en réalité une fonctionnalité malveillante. La sournoiserie avec laquelle il s'insinue nous semble faire de lui le modèle même de la cybercriminalité en général qui trahit notre vigilance.

634. Le terme est appliqué à cette menace informatique depuis 1970 et grâce à Daniel J. Edwards, un célèbre chercheur américain,qui l'a popularisé. Il dissimule le mal dans ses flancs. Le cheval de Troie, comme celui de la légende grecque, est en fait le véhicule dans (et par) lequel l'élément dangereux et nocif infecte un ordinateur.

Ce n'est pas le cheval lui-même qui est dangereux, c'est qu'il contient. La venue d'un cheval de Troie dans un système informatique peut se faire de bien des manières. Ce qui le rend justement si redoutable. Citons le téléchargement de versions trafiquées, sur des sites non

officiels ou des plateformes peu sûres, ou encore les pièces-jointes qui peuvent accompagner un courriel ; qu'il vaut mieux se garder d'ouvrir.

635. Il existe d'autres menaces analogues au cheval de Troie, comme l'injecteur (ou *dropper*) qui lui aussi sert de véhicule pour une malveillance. Il se présente comme un programme spécialement fabriqué pour propager des parasites, alors qu'il fait l'effet contraire.

La porte dérobée (backdoor), quant à elle, est un programme qui va s'exécuter discrètement sur l'ordinateur où il est installé pour y créer une faille de sécurité. Il peut ainsi accéder librement à internet et télécharger à l'insu de l'utilisateur, un parasite, qu'il ne véhicule pas en son sein contrairement au cheval de Troie. On peut dire qu'il lui ouvre simplement la porte. Quant au *Remote administration tool* ou RAT il s'agit d'un logiciel de prise de contrôle à distance d'un ordinateur, ce qui peut être légitime en certains cas extrêmes, mais peut aussi servir à un pirate pour s'emparer d'une machine, évidemment à l'insu de l'utilisateur. Il faut dire encore un mot des bombes de décompression qui ne transportent pas de parasite, mais peuvent être néanmoins rapprochées des chevaux de Troie. Il s'agit en l'occurrence d'un fichier compressé, qui, au moment de sa décompression, va générer un fichier d'une taille gigantesque qui pour cette raison va conduire au ralentissement ou même au plantage de l'ordinateur, et saturer le disque dur, lors même que ces bombes ne transportent aucun parasite indépendant.

636. La cybercriminalité se répartit en trois grands types : la cybercriminalité individuelle, la cybercriminalité contre la propriété et la cybercriminalité gouvernementale. Les types de méthodes utilisées et les niveaux de difficulté varient bien entendu selon la catégorie.

La cybercriminalité individuelle désigne en particulier la conduite d'une personne qui distribue des informations malveillantes ou illégales en ligne. Elle recouvre diverses formes de cyberharcèlement, mais aussi de distribution de pornographie (y compris infantile ce qui est beaucoup plus grave) et de trafic.

La cybercriminalité contre la propriété est - hélas - de plus en plus fréquente. L'un des cas les plus fréquents est celui de la captation, par un criminel, des coordonnées bancaires ou de la carte de crédit d'une personne physique ou morale pour accéder à ses fonds, faire des achats en ligne ou lancer des arnaques par hameçonnage (que l'on appelle aussi *phising* en anglais). Il s'agit d'une technique extrêmement utilisée pour obtenir des renseignements, en jouant sur la crédulité des victimes. Elle consiste à faire croire à la victime qu'elle est en relation avec quelqu'un (personne, organisme) de confiance et dans un cadre sécurisé. Elle peut, ainsi, lui

dérober, jouant d'un effet de surprise, des renseignements personnels et confidentiels par exemple des mots de passe, mais aussi des numéros de carte de crédit, une copie de la carte d'identités ou d'autres renseignements qui lui sont utiles à des fins bien entendu criminels. Parfois c'est un papier à en-tête qui est reproduit voire un site Internet complet qui est réalisé. Quelquefois, le travail est très grossier, mais ce n'est pas toujours le cas, hélas. Des personnes plus vulnérables, par exemple âgées et moins rompues aux arcanes de la cyberdélinquance tombe ainsi facilement dans le piège.

Souvent, on envoie aux victimes potentielles un message lui faisant croire que son compte courriel est désactivé. En effet, il est toujours profitable de jouer sur l'effet de surprise, de peur ou de panique. On parle alors souvent d'une « rupture de pattern », autrement dit la rupture d'une continuité psychique ; d'une séquence habituelle qui désarçonne la personne, ouvre une brèche et la vulnérabilise. De sorte qu'elle va faire une bêtise qu'elle n'aurait peut-être pas faite en temps ordinaire. Il est à noter que cette rupture de pattern est utilisée également en hypnose et qu'elle a fait ses preuves.

637. Bien entendu, ces techniques sont tellement éprouvées que même des personnes vigilantes peuvent se laisser prendre. De plus en plus, un hameçonnage systématique est réalisé par courrier électronique. Parfois, en faisant miroiter un gain ou un remboursement d'impôts. Certains sites sont bien entendu les cibles privilégiés de ceux qui pratiquent l'hameçonnage comme les services bancaires en ligne, les fournisseurs d'accès à l'Internet, les sites de ventes aux enchères tels qu'eBay, et le système de paiement Paypal.

638. Pour une vraie rentabilité, les escrocs s'adressent à de nombreuses victimes potentielles. Le phising, connaît plusieurs variantes, aussi pernicieuses les unes que les autres. On parle de *spear phising* pour l'hameçonnage sur des réseaux sociaux, mais aussi d'in-session phising lorsqu'on tente de récupérer la session utilisateur pendant la navigation, ce qui suppose une faille sur le site visité.

639. Il existe de nombreuses manières de conjurer un tel risque. Il est également possible et souhaitable de conjuguer les stratégies défensives. La première règle est celle de la vigilance la plus absolue de façon générale ; l'attention portée aux plus petits détails. Ainsi, il faut remarquer la syntaxe défaillante, le caractère inadéquat de l'adresse web proposée avec soin. On sait, en effet, que pour endormir la vigilance de l'internaute et lui inspirer confiance, les délinquants utilisent bien souvent un nom de domaine très semblable (mais évidemment pas exactement identique), parfois à un caractère près.

640. Les escrocs mettent au point des méthodes plus efficaces. Notamment celle qui consiste à masquer le nom de domaine effectif par l'utilisation de caractères habilement choisis parmi les dizaines de milliers de caractères du répertoire Unicode4. Certains caractères spéciaux présentent, en effet, l'apparence des caractères de l'alphabet latin. Pour éviter une telle arnaque, il n'y a qu'une seule solution qui consiste à ne pas permettre l'affichage de caractères qui ne sont pas inclus dans le répertoire ASCIL (lequel, on le sait ne comporte que les lettres de A à Z, les chiffres et les signes de ponctuation).

Pourtant, il est très difficile, aujourd'hui, d'avoir recours à une telle parade. En effet, elle ne s'accorde pas avec l'internationalisation des noms de domaine, supposant un répertoire bien plus large. Toutefois, il existe, depuis les années 1990, un moyen de lutte contre l'hameçonnage plus efficace et à plus large échelle, à savoir le certificat électronique. Il est vrai que pendant très longtemps l'interface utilisateur des navigateurs n'a pas permis de permettre aux utilisateurs comment accéder à cette parade. Cette interface se présentait sous la forme d'un petit cadenas. On se contentait souvent de dire aux surfeurs du net que ce cadenas signifiait simplement que la communication était chiffrée, ce qui bien entendu est vrai. Depuis, l'amélioration de la fabrication des certificats permet d'afficher plus clairement l'identité vérifiée d'un site.

641. Plus simplement, il est toujours recommandé d'écrire manuellement les adresses web complètes ou URL (plutôt que de taper sur un lien, qui peut en réalité être frelaté). Bien entendu, en amont, il est important que chacun connaisse des règles très simples au moins pour éviter de tomber dans des pièges grossiers. Par exemple, il est évident que les sociétés bancaires n'utilisent pas le courriel pour aborder un problème de sécurité avec des clients.

De façon générale, il est bon de faire suivre un message suspect à la société concernée. Sans doute, des filtres anti-spam aident-ils à protéger l'utilisateur des criminels informatiques, par le fait qu'ils réduisent le nombre de courriels que les utilisateurs reçoivent (et, par conséquent, les risques d'hameçonnage).

642. Les banques utilisent une identification renforcée. En France, par exemple, les internautes sont incités à communiquer avec la cellule de veille de la police nationale. Depuis 2010, il existe aussi une association à but non lucratif Phishing Initiative qui aide l'internaute à signaler les sites frauduleux dans le but de les bloquer. Les attaques sont devenues de plus en plus perfectionnées et passent aujourd'hui par les SMS (on les appelle alors *smishing*).

643. Il paraît, en tous les cas, judicieux de formuler une première observation : indépendamment d'une politique globale de lutte contre la délinquance, à large échelle, et en amont, le combat contre la cybercriminalité passe d'abord par des initiatives privées et individuelles ; par les parades que chaque victime concernée et potentielle peut veiller à mettre en place.

La lutte « macro » suppose le relai de la lutte « micro ». A cet égard, il est important de souligner que ce sont souvent les conduites imprudentes et irréfléchies des victimes qui incitent les escrocs à agir. De même que ce sont des imprudences qui favorisent le nombre de pickpopckets dans des métros ou ailleurs. Car ils tendent pour ainsi dire la main aux criminels.

644. Sans doute, la vigilance accrue des victimes potentielles risque ensuite par contre-coups de pousser les escrocs à mettre sur pied des stratégies plus retorses et plus sophistiquées. La lutte contre la cybercriminalité, avant de définir et d'affiner des politiques d'ensemble, avant de constituer une stratégie de répression, passe par à la base par la prise de conscience de chacun des agents concernés des risques encourus, des bonnes pratiques à adopter, des réactions et des parades à connaître. Ceci, dans leur propre intérêt, ainsi que dans l'intérêt de tous.

645. La cybercriminalité contre le gouvernement est moins répandue, mais il s'agit d'une forme de criminalité particulièrement grave. Elle peut avoir des conséquences importantes, à très large échelle. Nous y reviendrons plus loin, à propos de la cyberdéfense.

En effet, il y a lieu de parier que dans un monde où les tensions se multiplient (mais surtout se durcissent) ; où les Grands comme la Chine et les Etats-Unis sont dans une posture constante de bras de fer ; où des initiatives comme celle d'Israël d'annexer de façon unilatérale la Cisjordanie crée une menace beaucoup plus forte encore et plus imminente, les gouvernements vont de plus en plus souvent être pris pour cibles.

646. Ils ne vont pas seulement être pris pour cibles de l'étranger, mais peut-être aussi au sein du pays même, par des opposants déterminés. Le contexte actuel social de la France n'est pas des plus rassurants à cet égard. Cette cybercriminalité contre un gouvernement comprend en particulier le piratage de sites Web gouvernementaux, de sites militaires ou la diffusion de propagande.

Les criminels qui s'y adonnent sont habituellement des terroristes. Ils disposent d'un savoir-faire, de techniques, de matériaux et de moyens financiers considérables. Parfois, il s'agit de fous psychopathes, qui ne sont pas pour autant dénués de ruse et de constance. Nous y reviendrons plus loin de façon détaillée lorsque nous prêterons une attention particulière au terrorisme.

647. Du point de vue de l'inventaire - plus concret et plus précis - des différentes formes de criminalité, il est intéressant de donner quelques détails plus techniques, pour mieux comprendre ce dont il s'agit. Ceci, afin de mieux cerner les enjeux, et par là imaginer des parades.

Il faut mentionner d'abord les attaques dites DDoS qui servent à rendre un service en ligne indisponible et à détruire le réseau en submergeant le site de trafic provenant de diverses sources. Sont alors créées de vastes réseaux d'ordinateurs contrôlés de l'extérieur, par des pirates informatiques à distance. Les pirates envoient ensuite des spams ou attaquent encore d'autres ordinateurs, par le biais de ces botnets. Ces mêmes *botnets* peuvent également être utilisés pour agir en tant que virus et effectuer des tâches malveillantes. Tout cela passe par l'envoi de logiciels malveillants sur les ordinateurs des utilisateurs. Lorsque le réseau est en panne, c'est tout le système qui est infecté.

648. Le vol d'identité est également un acte fréquent et très grave de cybercriminalité. Un criminel parvient à obtenir l'accès aux informations personnelles d'un utilisateur, pour lui voler de l'argent, ou mettre en œuvre quelque fraude que ce soit, y compris ouvrir un compte téléphonique ou un compte Internet au nom d'une malheureuse victime escroquée. À cet effet, les pirates s'emparent des mots de passe, volent des données personnelles sur les réseaux sociaux.

649. Le *cyberstalking* constitue une sorte de harcèlement en ligne. Le malheureux internaute qui en est victime est soumis à un très grand nombre de messages en ligne ou directement par mail. Ce harcèlement se sert en particulier des réseaux sociaux, des sites web et des moteurs de recherche. L'arme la plus efficace est la peur. Toutefois, elle est renforcée par la répétition de l'agression.

650. L'ingénierie sociale quant à elle relève de pratiques de manipulation psychologique, bien entendu à des fins d'escroquerie et dans des buts lucratifs. Les criminels, en général, contactent directement leurs victimes par téléphone ou par mail. Ils tentent bien entendu de gagner la confiance pour parvenir à leurs fins. Ainsi, ils peuvent se faire passer pour des agents du service public, afin de se faire fournir des informations dont ils ont besoin. Le genre d'informations concerné est le mot de passe, ou le nom de l'entreprise ou encore les coordonnées.

651. Les criminels tentent de s'en prendre à leurs amis sur Facebook, par exemple, en leur demandant de les ajouter comme ami. Il s'agit d'inspirer confiance, mais quelquefois un autre stratagème

est employé, celui du sexe. Des personnes peu vêtues ou aguichantes invitent des « pigeons » éventuels à les prendre pour ami sur Facebook.

652. Les Programmes Potentiellement Indésirables que l'on appelle aussi PUPs (en raison de leur appelation anglaise Potentially Unwanted Programs). S'ils sont moins redoutables, ils n'en sont pas moins vraiment malveillants. Ils désinstallent les différents logiciels du système de l'utilisateur Internet, mais aussi les moteurs de recherche et les applications pré-téléchargées. Parfois, ils introduisent des logiciels pirates, espions ou publicitaires. Il existe un autre genre de pratique illégale en ligne, qui consiste dans le partage et la distribution d'un contenu non autorisé et inapproprié. Qui peut parfois être très pénible et offensant.

653. Nous en reparlerons au sujet de personnalités publiques, qui ont vu leur réputation démolie suite à la publication, même éphémère et rapidement retirée, d'une vidéo les présentant dans situations gênantes y compris pornographiques. Il peut aussi s'agir de vidéos ou de photos d'une extrême violence, montrant par exemple des meurtres. Les kits d'exploitation peuvent aussi attaquer un ordinateur et en prendre le contrôle. Ce sont des outils faciles à utiliser et que l'on peut acheter clés en main. Néanmoins, ils ne peuvent s'introduire qu'au bénéfice d'une vulnérabilité dans un ordinateur, en l'occurrence un bug. Ces redoutables kits d'emploi sont régulièrement mis à jour, comme n'importe quel logiciel normal. Ils sont disponibles sur des forums de piratage sur le web. Cette diversité suppose certes des principes généraux pour les combattre, mais également des normes spécifiquement adaptées à chaque cas. La criminalité semble bien accompagner la vie des hommes depuis toujours semble-t-il[433]. Néanmoins, les diverses formes de criminalité correspondent toujours à un contexte et aux moyens d'une époque.

654. Il est intéressant, par exemple, de voir la récurrence de la piraterie au travers des siècles[434]. La piraterie constitue une forme singulière redoutable de criminalité, au détriment des biens et des personnes, souvent prises en otages ou massacrés.

Elle exprime une certaine cohérence d'ordre économique (à défaut d'être éthique !) qui a été étudié au XXe siècle[435]. Au départ, l'étymologie du mot « pirate » est méliorative et positive.

---

[433] Xavier ROUSSEAUX, *Violence, conciliation et répression: Recherches sur l'histoire du crime, de l'Antiquité au XXIe siècle,* Louvain, Presses Universitaires de Louvain , 2013.

[434] Très vaste bibliographie : Gilles LAPOUGE, *Les pirates*, Paris, Balland, 1969; Jean-Pierre MOREAU, *Une histoire des pirates*, Paris, Points Histoire, 2007 ; Marcus REDIKER*, Les Hors-la-Loi de l'Atlantique. Pirates, mutins et flibustiers*, Paris, Seuil, 2017.

[435] Serge SCHWEITZER, « Economie de la piraterie » in *Contrepoints* : *https://www.contrepoints.org/2020/03/22/366494-histoire-des-idees-economiques-economie-de-la-piraterie-29*

Le *pirata* latin (les noms de métiers, curieusement, en latin sont en –a et féminins) est celui qui tente la fortune, qui est entreprenant, qui se présente comme industrieux, comme un chevalier d'industrie. Toutefois, le mot grec est plus péjoratif. Il désigne un brigand qui navigue sur les mers. On note une certaine ambivalence dans l'appréciation. D'une part, le pirate est mal considéré, car il est un escroc. Il commet des forfaits et des meurtres. De l'autre, il fascine par son habileté et fait envie par sa vie aventurière et libre.

655. Si les corsaires se livrent souvent à une activité semblable, c'est avec l'aval des autorités de leur gouvernement. D'une certaine façon, la piraterie se différencie par une volonté de s'affranchir des règles et des limites. Il y a aussi des codes d'honneur qu'ils respectent quelquefois. On ne peut pas dire qu'ils sont sans foi ni loi. Au contraire. Ils suivent une foi et une loi qui ne sont pas celles de leur État. Si, au départ, le pirate sévit sur les routes en voleur de grand chemin, aujourd'hui il sévit sur les autoroutes informatiques. L'appellation « pirate de l'air » n'est du reste pas très heureuse. Il s'agit de terroristes. Les vrais pirates ne sont pas des terroristes, mais des criminels de droit commun. Quant aux bio pirates, dont on parle depuis peu, ils manipulent le vivant en dehors de tout cadre légal, souvent dans des laboratoires clandestins[436].

656. D'une certaine manière, " les pirates sur mer " sont des héros, car ils mènent une vie très difficile et périlleuse ; bien plus en tout cas que celle de nos pirates informatiques. Le piratage informatique se présente comme une forme de piraterie sans trop de risques (notamment physique pour nos nouveaux pirates), en tout cas jusqu'à présent.

657. La Poste a souvent été la victime de pirates cherchant à s'approprier des secrets, par curiosité ou pour faire du chantage, mais également pour s'emparer d'éventuels billets de banque qui se trouveraient dans des enveloppes (ou autres objets précieux). A la fin des années 1960 et au début des années 1970, c'est le téléphone qui est régulièrement piraté ; avec l'apparition des premiers téléphones électroniques.

658. Des experts en technologie que l'on connaît sous le nom de *phreakers* ont alors trouvé un moyen de payer des appels longue distance grâce à une série de codes frauduleux. On peut donc les considérer d'une certaine façon comme les premiers pirates. Dont le but, sans doute moins effrayant, était de voler du temps de téléphone longue distance. Le premier pirate de nouveau genre est le célèbre capitaine Crunch (de son vrai nom John Draper) qui a réussi à utiliser un

[436] Vandana SHIVA*, Biopiracy. The Plunder of Nature and Knowledge,* South Yarra, South Press, 1997.

sifflet trouvé dans une boîte de céréales Captain Crunch – d'où son sympathique surnom - pour accéder à des fonctions spéciales de la centrale téléphonique.

659. En France, un tout petit peu plus tard, au début des années 1970, des chercheurs ont remarqué qu'en déclenchant du doigt un très bref raccrochage pendant quelques centièmes de seconde, le standard l'interprétait comme un 1, sans passer par le testeur de numéros, ce qui permettait d'avoir gratuitement accès au téléphone international. Par la suite, ce sont les télécartes qui furent l'objet de piratage pendant les années 1990. A chaque fois, des parades ont été trouvées. Ainsi, France Télécom met en circulation un nouveau type - mieux sécurisé - de télécartes, avec un nouveau système de chiffrement. De nombreuses autres escroqueries se sont multipliées au fur et à mesure que de nouvelles techniques étaient mises en place.

660. Avec le développement des nouvelles technologies et l'apparition de l'Internet, les techniques de piratage téléphonique sont désormais obsolètes et les pirates s'attaquent à d'autres choses. Nous pouvons à nouveau faire la même observation : au fur et à mesure du progrès des parades pour les contrer, les pirates inventent d'autres attaques et imaginent d'autres scénarios, faisant ainsi preuve d'une imagination toujours renaissante. Cela rend d'autant difficile - et peut-être exaltante aussi - la tâche de celui qui entend les combattre et les vaincre. Même si ce n'est peut-être jamais que pour un temps.

e. Des menaces d'envergure croissante

661. En 1990, un grand projet (du nom d'opération Sundevil[437]) a été lancé pour lutter contre un nouveau type de criminalité. Il s'agit d'une opération des Services secrets étatsuniens conduite à l'échelle nationale contre des "des activités illégales de piratage informatique".

    Ce plan de lutte contre l'escroquerie informatique incluait des perquisitions dans une quinzaine de villes, des arrestations et des confiscations d'ordinateurs. Au-delà de l'efficacité directe de cette action, il s'agissait de marquer les esprits et d'adresser un message d'avertissement à tous les pirates potentiels.

662. Le message délivré voulait également leur signifier que l'anonymat relatif des terminaux électroniques ne sauraient les protéger. Pour que le message passe, il fallait évidemment une large médiatisation. En définitive, dans toute chose, il y a bien une part de « Comm », comme

[437] Le nom de cette opération vient om vient du stade de football Sundevil de l'Arizona State University, où siégeaient les services secrets locaux.

l'on dit aujourd'hui. De fait, il semble que ce projet ait, au moins pendant un certain temps, freiné l'audace des pilates, au moins dans une large mesure.

À long terme, les pirates ont imaginé d'autres façons d'agir et d'autres parades. Sur le coup, l'opération Sundevil se caractérise donc bien par un certain succès tactique. Toutefois, indirectement, il a contribué à un affinement et à une meilleure efficacité des techniques de piratage.

663. C'est également en 1990 qu'a été fondée l' « Electronic Frontier Foundation »; en vue de répondre aux menaces qui pouvaient peser sur les libertés publiques. Il s'agissait de défendre les consommateurs contre des poursuites illégales et des abus de la part des forces de l'ordre.

Cette fondation est une Organisation non gouvernementale internationale de protection des libertés sur internet basée à San Francisco en Californie et fondée par Mitch Kapor, John Gilmore, et John Perry Barlow. Ce dernier, militant libertarien, est - du reste - l'auteur de la Déclaration d'indépendance du cyberespace. Il entend lutter contre toute forme de censure et de limitation des libertés.

D'emblée, une observation importante peut donc être faite. La marge entre le contrôle légitime de l'Internet, pour lutter contre la criminalité et l'empiétement sur les libertés, n'est pas facile à évaluer. Son appréciation relève souvent des convictions philosophiques des uns et des autres. La lutte contre la criminalité informatique peut-elle vraiment légitimer certaines restrictions en matière de libertés individuelles ?

664. À nouveau, il semble que nous nous trouvions, comme pour beaucoup de questions rencontrées dans notre recherche, confrontés à une sorte de conflit entre deux exigences opposées. Le législateur et l'exécutif doivent-ils alors parvenir à une sorte de point d'équilibre ? Mais comment ?

Ce questionnement est constant tout au long de notre travail. Ainsi, cette association, qui naît l'année-même de l'opération Sundevil, témoigne de la difficulté de mener une action vigoureuse policière et juridique ; dans la mesure où combattre le piratage risque de menacer des libertés légitimes. Dès 1990, *l'Electronic Frontier Foundation* organise des actions politiques et l'envoi de courriels en masse. Elle avance des fonds pour la défense dans les procès, car elle estime que la défense des principes de libertés est une cause d'une importance fondamentale. Elle défend aussi les individus et les nouvelles technologies contre le risque que ne s'établisse une société de surveillance et de contrôle. L'action de cette organisation a cependant été vivement controversée. On lui a reproché de couvrir les hackers.

665. Le développement du *Darknet*[438] - en fait un ensemble de réseaux que l'on appelle chacun *darkne*t avec une minuscule - a rendu le problème plus crucial encore. On sait qu'il s'agit d'un réseau superposé, qui se sert de protocoles bien spécifiques, avec des fonctions d'anonymat. Ce réseau superposé permet des opérations diverses : comme l'échange de fichiers, ou la construction d'un écosystème anonyme complet comme Freenet. Sa spécificité réside bien dans l'anonymat : à savoir, que les adresses IP ne sont pas révélées et que les utilisateurs sont donc à même de communiquer sans grande crainte d'être contrôlés part des gouvernements, ou des entreprises.

666. Cette protection de l'anonymat, qui peut sembler un gage d'impunité, explique bien pourquoi les réseaux d*arknets* sont prisés pour les dissidents politiques, de même que tous ceux qui s'adonnent à des activités illégales. Ils forment un certain univers *underground*, permettant d'y déployer des activités qui ne peuvent paraître au grand jour, d'où l'usage de l'adjectif « *dark* ». De même qu'on appelle « travail au noir », celui qui fait un travail rémunéré qui ne doit pas apparaître au grand jour car il n'est pas légal. De même qu'on appelle «nègre » celui qui écrit un livre pour un autre, ce qui ne doit pas davantage apparaître au grand jour. Le terme *Darknet* apparaît au cours des années 1970, pour désigner des réseaux isolés du futur Internet. Les adresses n'apparaissaient pas dans les listes de réseaux et n'étaient pas identifiables. Le terme émerge véritablement en 2002, suite à un article rédigé par quatre employés de Microsoft[439]. Le terme n'a alors pas tardé à se répandre comme une traînée de poudre et être connu du grand public.

667. Par exemple, en septembre 2013, en France, le magazine de télévision *Télérama* publie un dossier de vulgarisation, intitulé « Darknet : immersion en réseaux troubles »[440]. L'année 2013 est une année importante à cet égard car le terme y est souvent employé et ce choix terminologique commence à susciter des polémiques. Derrière la diabolisation du Darknet, il y aurait des intérêts occultes de puissantes entreprises comme Google et Facebook, qui font un commerce lucratif des données personnelles de leurs usagers. L'indignation morale serait donc en partie un prétexte.

---

[438] Jean-Philippe RENNARD, *Darknet : mythes et réalités*, Paris, Ellipses, 2016 ; Rayna STAMBOLIYSKA*, La face cachée d'internet : hackers, darknet…*, Paris, Larousse, 2017.

[439] Peter BIDDEN, Paul ENGLAND, Marcus PEINADO et Bryan WILLMAN , « The Darknet and the Future of Content Distribution » sur le site *msl1.mit.edu.*

[440] *http://archive.wikiwix.com/cache/?url=http%3A%2F%2Fwww.telerama.fr%2Fmedias%2Fdarknet-immersion-en-reseaux-troubles%2C102055.php*

668. On le voit encore, dans la question de la lutte contre les pratiques illégales, quand il s'agit de l'Internet, rien n'est simple. Nous ne sommes pas dans le domaine du tout blanc ou du tour noir. Ce qui peut contribuer à faire du mal peut contribuer aussi à faire du bien, comme le *Pharmakon* des Grecs. Le juriste doit donc se garder du jugement et privilégier un discernement à la fois prudent et vigilant.

La diabolisation du *Darknet* pourrait faire partie d'une stratégie de surveillance globale des internautes, sans nier ce que ce darknet peut en effet avoir de dangereux. Bien entendu, on peut y trouver de célèbres supermarchés de la drogue comme la fameuse *Silk Road*. La *Silk Road* est un marché secret qui utilise un réseau bien spécifique, afin d'assurer l'anonymat et la protection de ses acheteurs et vendeurs (dans le cadre de la vente de produits illicites, en particulier de stupéfiants).

669. Le FBI a découvert le pot aux roses, en octobre 2013. Il a démantelé un premier site, mais une autre version, plus performante, a été rouverte seulement quelques semaines plus tard. Cela illustre bien la conviction selon laquelle combattre la cybercriminalité est comme le mythe de Sisyphe, qui pousse un rocher, lequel finit par dévaler la pente de nouveau. Dès lors qu'une parade est trouvée ou qu'une organisation est démantelée, la criminalité trouve toujours d'autres expédients. Le site opère lui-même une sorte de sélection, dans l'ensemble des trafics qu'il met en place. Ainsi, il interdit celui des cartes de crédit volées ou la pédopornographie. Il exclut aussi le trafic d'armes, beaucoup trop dangereux, qui se réalisait sur un site analogue, jusqu'à sa fermeture au bout de quelques mois.

670. En réalité *Silk Road* n'est aucunement un instrument de vente, mais une plateforme pour mettre en relation les vendeurs et les acheteurs. Il présentait ainsi un listing de produits aux acheteurs et offrait un système de paiement fondé sur un dépôt fiduciaire. Le montant de la transaction est en suspens en attendant l'arrivée effective du bien ou du service et le site s'occupait des différends éventuels. Il utilisait seulement une monnaie électronique séparée du système bancaire international, dont nous avons déjà parlé, le *bitcoin.*

671. Ensuite, les marchandises commandées (les stupéfiants) sont acheminées par les réseaux standards de distribution de courrier et colis. Cela se faisait sans trop de risques excessifs. En effet, il n'était pas possible (aussi bien pour des raisons pratiques et déontologiques) de fouiller tous les colis, ou de vérifier toutes les identités des expéditeurs.

672. Enfin, si jamais un colis était découvert, son destinataire ne saurait être incriminé pour le fait même que n'importe qui pouvait recevoir un colis sans en être responsable. Cette technique est

fortement utilisé en matière de trafic de stupéfiants. Pour démanteler *Silk Road,* il a été nécessaire de mobiliser une centaine d'agents fédéraux, travaillant évidemment sous couverture, mais le succès a fini par se trouver au rendez-vous.

En effet, une drogue d'une grande pureté a été découverte en grande quantité à destination de dix pays européens, générant des ventes très lucratives ; avec un commission très substantielle de 80 millions d'euros, au bénéfice de *Silk Road*. Son fondateur, un quidam nommé Ross Ulbricht, a été condamné à une peine de réclusion à perpétuité.

673. La justice américaine ne plaisante pas. Cependant, la résurgence presque immédiate de *Silk Road* montre que telle une hydre dont la tête repousse après avoir été coupée la cybercriminalité se reconstruit rapidement après son démantèlement. Ce qui est rassurant c'est qu'en novembre 2014 le fondateur du site Blake Benthall a été arrêté .

674. Finalement des sites du même genre ont disparu en 2017. Ce qui ne veut pas dire la disparition du Darknet pour autant, bien entendu. Sur le *Darkne,t* on trouve en effet des ventes d'armes et des tueurs à gage. L'utilisation présumée dans des intentions terroristes justifie une attention accrue. Néanmoins, le *Darknet* n'est pas seulement au service de la criminalité. Il permet également à des journalistes, par exemple ceux appartenant à « Reporters sans frontières » de protéger des envoyés spéciaux en temps de guerre ou dans des pays peu respectueux des droits de l'homme ou des libertés fondamentales. Il faut savoir aussi – toujours en positif - que le *Darknet* est utilisé par des lanceurs d'alerte et par des dissidents qui entendent se protéger de la surveillance de masse. Il permet également à des personnes accusées dans certains pays de comportements déviants, comme les homosexuels, d'échapper à des poursuites et à des persécutions. Enfin, de façon plus anodine sans doute, le *Darknet* sert aussi à partager des fichiers avec des personnes de confiance, et ainsi à un échange entre personnes qui veulent bénéficier d'une plus totale confidentialité. Ce qui est tout-à-fait légitime dans la mesure où ils ne commettent pas d'actions illégales et n'agissent pas dans des buts illégaux.

675. Au début, le logiciel *Apple iTunes* autorisait, du reste, ses utilisateurs à s'assigner une adresse IP d'un réseau distant et à partager ainsi leur musique avec les autres utilisateurs du réseau non légal. Encore une fois, les réseaux du *Darknet* et ses utilisateurs ne sont pas forcément animés par des intentions criminelles. Cela confirme l'observation que nous avons déjà formulée, à plusieurs reprises, d'une ambivalence des nouvelles technologies et de ses ressources. Autre exemple, le logiciel *Syndie* permet d'utiliser et de mettre en service des forums et blogs anonymes afin que ceux-ci ne soient pas censurés. On peut y voir une manière de sauver la liberté d'expression, éthiquement acceptable, ou même digne d'être louée.

676. De toutes les manières, il existe des dizaines et des dizaines de réseaux darknet, fort différents quant aux finalités qu'ils s'assignent, mais également par leur fonctionnement. Certains d'entre eux comme Tor réussissent à fédérer de très importantes communautés. Ainsi, Tor20 se présente comme une forme de mixnet qui s'est développée au début des années 2000 par l'armée américaine. Il regroupe quotidiennement, pas moins de 2 millions d'utilisateurs. Ce qui est considérable, aussi bien intéressés par des marchés noirs que par des sites d'expression politique en toute liberté. Freenet22 propose quant à lui un écosystème anonyme et complet, principalement dans la perspective de libres échanges ou de libres projets d'ordre politique.

Une attention particulière peut aussi être accordée au *Telegram messager* qui vise notamment à court-circuiter la censure exercée en Russie. L'anonymat des dissidents est ainsi protégé et un recrutement discret peut avoir lieu.

677. Le *Darknet* rassure donc – peut-être prématurément et à trop bon compte – des dissidents ou des escrocs qui craignent ou la police ou les indiscrétions. Néanmoins, le secret du *Darknet* n'est pas si absolu, ni si impénétrable que cela. Si une opération de grande envergure est menée pour y démanteler certains réseaux, cela s'avère en général efficace. Par ailleurs, le *Darknet* n'échappe évidemment pas aux bugs informatiques et aux erreurs d'utilisation par un utilisateur. Il peut y avoir aussi une erreur de paramètre dans un logiciel ou encore un problème de matériel. Tout cela reste marqué au sceau de la vulnérabilité. Les grands cybercriminels sont hautement qualifiés et difficiles à trouver. Cela demande un important moyen de combat, tant en hommes que financiers. Les gains potentiels des criminels sont considérables. Ce qui explique leur multiplication, et la généralisation de la cybercriminalité. De sorte que personne n'est à l'abri et qu'une sécurité d'un moment ne constitue guère une garantie pour le futur. De plus, s'il n'est pas facile de détecter une cyberattaque, cela prend surtout beaucoup de temps ; sauf cas d'une escroquerie immédiate dont serait victime un particulier.

678. Une entreprise met ainsi plus de 200 jours en moyenne, soit la moitié d'une année, pour mettre un terme à une attaque subtile, sophistiquée et sournoise. La cybercriminalité est favorisée par le fait qu'un certain nombre d'internautes ne sont pas très prudents et ne changent pas leurs mots de passe ou alors en prennent de trop simples faciles à craquer.

679. À une cybercriminalité presque artisanale (mais avec des effets considérables en raison du nombre de personnes attaquées dont certaines finissent par se faire avoir), se superpose ainsi une cybercriminalité beaucoup plus élaborée et efficace (visant des personnes morales et non des individus) dont les buts sont variés.

680. En 2013, aux Etats-Unis, les magasins TARGET ont été sérieusement touchés par le piratage géant de données, qui a pu atteindre jusqu'à 100 millions de clients, à savoir un américain sur trois. De nombreuses informations de clients ont été dérobées : comme les noms, les adresses postales, les numéros de téléphone ou les adresses e-mail. Cela a justifié une enquête d'ampleur nationale et des contreparties offertes aux clients, comme : un an de surveillance de crédit et de protection contre le vol d'identité électronique à tous ses clients ayant fait des achats aux États-Unis. Il s'en est suivi une perte de confiance envers la chaîne Target. D'ailleurs, la volonté de nuire à une entreprise ou à une chaîne peut, au-delà de l'intérêt propre des données volées, expliquer une attaque, dont elle constitue au moins la conséquence, sinon le but.

681. Les cerveaux de telles attaques sont souvent géographiquement très loin du siège d'un groupe impacté. En l'occurrence, en ce qui concerne les attaques des magasins TARGET, ils se trouveraient en Europe de l'Est, où la criminalité informatique est très développée, on le sait. En 2015, TV5 Monde subit un autre type d'attaque à savoir visant non un vol mais un blocage. En effet, cette attaque de grande ampleur entraîne entre les 8 et 9 avril 2015 l'arrêt de la diffusion des programmes de la chaîne de télévision francophone internationale TV5 Monde, avec un parasitage particulièrement déplaisant, en l'occurrence des messages de soutien à l'État islamique.

682. Cette action est revendiquée par le groupe de pirates informatiques « Cybercaliphate », qui se réclame de l'organisation État islamique ; alors même que ce dernier n'a pas confirmé l'information. Les enquêteurs suspectent cependant des hackers russes regroupés sous le sigle APT28 (ou Pawn Storm), et peut-être appuyés en sous-main par le gouvernement russe.

683. Il convient également de se souvenir que, dès février 2012, face à la recrudescence des cyberattaques, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) lance en France un exercice dans le cadre du plan Piranet visant à « mettre l'État français à l'épreuve d'une crise informatique majeure ».Le scénario consiste en une attaque de grande ampleur de l'Internet français et des réseaux des administrations pour tester la capacité de l'État à réagir et à se coordonner ; en ne se laissant pas trop désarçonner par l'effet de surprise. Des représentants des secteurs les plus vitaux pour la vie du pays comme la santé, les transports et les communications électroniques participent à ce plan.

684. À peine trois ans plus tard, dans la semaine qui suit les attentats de janvier 2015 en France, 19 000 sites internet français sont attaqués par des groupes qui revendiquent la « Défense des musulmans » et la cause propalestinienne. Cette vague d'attaques informatiques s'en prend

surtout aux sites de petites collectivités territoriales ou de PME, évidemment plus vulnérables, et tous reliés par une même série de serveurs informatiques.

685. Par ailleurs, à la même période, le 12 janvier 2015, les comptes Twitter et YouTube du commandement de l'armée américaine au Moyen-Orient et en Asie centrale (CentCom) sont piratés par un groupe de hackers prenant le nom de « Cybercaliphate ». Quelques jours plus tard, toujours pour provoquer un effet de harcèlement et d'exaspération, le site Internet et le compte Twitter du quotidien français Le Monde sont la cible de plusieurs attaques de l'Armée électronique syrienne. Pourtant, solides et très au point, les mécanismes de sécurité du journal, résistent bien.

686. Le 10 février 2015, c'est le compte Twitter de l'hebdomadaire américain Newsweek qui est victime d'une attaque par le Cybercaliphate. La revendication du terrorisme islamiste pouvant offrir un prétexte et une couverture. L'enquête menée confirme du reste cette piste, car l'attaque présente une ressemblance avec le mode d'un réseau de hackers russes.

687. De plus, le code source aurait été tapé sur un clavier cyrillique à des moments qui correspondent aux heures de bureau à Saint-Pétersbourg et à Moscou. Enfin, le contexte extérieur est celui d'une dégradation des relations entre la France et la Russie à la suite de la suspension de la livraison de deux navires Mistral sur fond de crise ukrainienne. L'attaque de TV5 Monde ne relève, en tout cas, en rien du hasard. On sait cette chaîne de télévision, généraliste, francophone et surtout internationale, créée le 2 janvier 1984 et détenue conjointement par des sociétés audiovisuelles publiques françaises, belges, suisses, canadiennes et québécoises, constitue bien l'un des trois plus grands réseaux mondiaux de télévision, accessible auprès de 291 millions de foyers, à travers 200 pays et territoires. L'attaquer présente donc un intérêt stratégique tout-à-fait évident.

688. A la fin du mois de mars 2015, alerte est donnée par des services de renseignement d'une potentielle utilisation frauduleuse d'un de ses serveurs non protégé. Finalement, et ce rapidement, un serveur vulnérable est identifié et la chaîne internationale se met à la recherche d'un prestataire pour un audit de sécurité. Peu de temps plus tard, le 8 avril 2015, TV5 Monde inaugure alors sa nouvelle chaîne thématique sur l'« art de vivre à la française », TV5 Monde Style HD, en présence du ministre des Affaires étrangères Laurent Fabius. Ce qui put attirer l'attention et créer l'occasion d'un enjeu d'attaque stratégique.

689. Il faut ainsi savoir que la chaîne diffuse du contenu au Moyen-Orient sur des sujets les plus variés. Ce même 8 avril au soir, à 20h50, l'infrastructure de diffusion de TV5 Monde (le

multiplexage) est la cible d'une cyberattaque. Dans un premier temps, les services compétents pensent à une simple panne technique. C'est alors que le serveur électronique est détruit. Ce qui confirme une cyberattaque, rapide et même fulgurante. Les diffusions de la chaîne sont alors interrompues.

690. Comme les meilleures attaques se font sur plusieurs fronts, en même temps, les comptes Twitter et Facebook de la chaîne sont eux aussi piratés. On y trouve des messages de soutien à l'État islamique en anglais, arabe et français, tout comme des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'Etat Islamique.

691. De façon très explicite, un message s'en prend aussi au président de la République François Hollande. Il est accusé d'avoir commis « une faute impardonnable » en menant « une guerre qui ne sert à rien ». Référence est également faite aux attentats de janvier 2015. Les propos sont terriblement menaçants : « Soldats de France, tenez-vous à l'écart de l'État islamique ! Vous avez la chance de sauver vos familles, profitez-en. [...] Au nom d'Allah le tout Clément, le très Miséricordieux, le CyberCaliphate continue à mener son cyberjihad contre les ennemis de l'État islamique ».

692. En peu de temps, fort heureusement, des équipes techniques arrivent à reprendre le contrôle des réseaux sociaux et postent des messages d'explication à destination du public dénonçant selon les termes du directeur général de TV5 Monde, Yves Bigot, une « cyberattaque extrêmement puissante ». Le bon fonctionnement de la chaîne reprend peu à peu le jour suivant. La direction générale de la Sécurité intérieure (DGSI), la sous-direction anti-terroriste (SDAT), et les cyber-policiers de la direction centrale de la Police judiciaire (DCPJ) sont saisis. Quant aux experts de l'agence nationale de la sécurité des systèmes d'information (ANSSI), ils sont chargés d'analyser le mode opératoire. Une brève enquête révèle bien entendu que cette attaque n'a pas pu être menée par un individu isolé mais par plusieurs dizaines de pirates singulièrement compétents, probablement des mercenaires, bien entendu rémunérés à prix d'or. De telles attaques supposent donc une base financière très consistante. Les pirates devaient d'ailleurs être infiltrés depuis des semaines dans les réseaux de TV5 Monde.

693. Ils ont utilisé la technique de l'hameçonnage (ou phishing) en envoyant un e-mail fin janvier à l'ensemble des journalistes de la chaîne. Trois d'entre eux ont commis l'imprudence de répondre, ce qui a permis aux hackers de pénétrer le réseau de la chaîne par le biais d'un cheval de Troie très habilement conçu. Trois semaines avant l'attaque proprement dite, un virus informatique s'est ainsi propagé dans plusieurs ordinateurs, profitant d'une architecture

informatique mélangeant la partie « métier » constituant le cœur de la chaîne et la partie bureautique ouverte sur l'extérieur via Internet. Les pirates peuvent alors circuler à leur guise dans tout l'espace internet de la chaîne. En tout cas, cette cyberattaque éveille les consciences des divers responsables sur les risques qui sont encourus. Il est décidé d'allouer des moyens plus importants à la cybersécurité ainsi que de créer 500 emplois supplémentaires.

694. Même si la chaîne a pu reprendre ses activités assez rapidement, pendant plusieurs mois, elle connaît d'importants problèmes de fonctionnement. Ainsi, les journalistes ne peuvent-ils pas accéder à l'intégralité du réseau informatique de la chaîne pendant plusieurs mois, ni utiliser le wifi et Skype, ni scanner des documents car le réseau Internet n'est pas encore reconnecté.

695. Les conséquences financières de cette attaque seraient d'environ 8 millions d'euros à court et long terme. De plus, la chaîne se voit obligée d'investir au moins 10 millions d'euros dans sa cybersécurité par la suite. La facture est donc salée. Toujours est-il qu'en 2015, des pirates de Rex Mundi, un groupe très structuré et très efficace s'en prennent à Labio, un laborabatoire d'analyse de sang, s'emparant de données médicales, choses particulièrement sensibles. Ce groupe de délinquants est bien connu dans le monde de la cybercriminalité car il multiplie les opérations, en particulier le chantage.

696. Sa technique favorite est d'extorquer la base clientèle d'entreprises spécialisées dans la finance pour exiger une rançon, brandissant la menace de la divulguer au grand public. Cela confirme, si besoin était, combien les données confidentielles sont aujourd'hui des biens précieux valant chers.

697. Leur divulgation au grand public est également singulièrement compromettante et pénalisante pour les sociétés comme pour leur clientèle, à plusieurs égards. En tout cas, ce même groupe Rex Mundi compte déjà à son actif, parmi d'autres, la banque franco-belge Dexia, une société belge d'intérim, une société américaine spécialisée dans le crédit Americash Advance, la société française Créditpret1 ou encore la société française Numéricâble. Comme on peut le constater, elle ratisse large.

698. Le 29 mai 2014, Rex Mundi déclare avoir piraté les données de 800 patients des serveurs de la société belge Xperthis, spécialisée dans les technologies de la communication des hôpitaux, mais ce piratage n'est pas confirmé et pourrait relever de l'esbrouffe. Ou alors, il pourrait s'agir de données vieilles de dix ans qui ont donc perdu beaucoup de leur intérêt. Ainsi donc le 17 mars 2015, les pirates de Rex Mundi rendent publiques les données médicales de 15 000 français après avoir exigé en vain une rançon auprès de Labio, laboratoire d'analyse de sang.

Cette divulgation choque profondément les consciences car il touche au domaine sensible de la santé et du secret médical.

699. Le secteur médical est peut-être, du reste, moins protégé que d'autres comme la grande industrie ou la défense alors même que les données qu'on y trouve sont de grande importance. Rex Mundi agit bel et bien dans la perspective d'une fraude, à savoir le monnayage d'informations subtilisées, faisant peser le chantage de leur divulgation. Cette attaque révèle une fois encore combien la question de la protection des données personnelles est importante et sensible.

700. Les cyberattaques peuvent s'attaquer à un État dans un but politique. C'est notamment le cas de l'attaque informatique de la centrale nucléaire de Bouchehr en Iran dans le but de dcétruire des centrifugeuses d'enrichissement d'uranium en 2010. Les réseaux informatiques de l'Etat géorgien ont également été détruits en 2007. Tout récemment encore, alors que se prolonge la sinistre pandémie du Coronavirus, l'Australie est victime d'une cyberattaque de grande ampleur dirigée contre le pays par un Etat voisin, mais sans qu'aucune preuve ne permette de l'accuser définitivement et nommément.

701. C'est la Chine qui est vivement soupçonnée mais comme toujours dans de semblables attaques il est difficile d'avoir une certitude absolue et donc plus encore d'accuser. C'est la sophistication de l'attaque et l'étendue de ses conséquences qui entretient la suspicion sur la Chine car il faut un pays en mesure de mener une semblable attaque. Les experts australiens relèvent des similitudes en comparaison avec d'autres attaques récentes, par exemple menées contre leur Parlement en février 2019.

702. Il est dès lors évident que face à telles menaces et à de telles attaques déjà en cours il faut trouver très vite des parades et opposer à cette prolifération de la délinquance une culture de la cybersécurité, à asseoir aussi bien du point de vue juridique que dans la pratique concrète et même quotidienne, notamment policière.

Section II : le droit au service de la cybersécurité

a. L'arsenal juridique

COMPLETER AVEC LES EMIRATS ET LES AUTRES GRANDS PAYS

703. La loi vise à protéger les droits des individus, même si elle leur assigne aussi des devoirs. Il y a d'ailleurs une inséparabilité des droits et des devoirs, qu'il serait illusoire d'occulter. Du reste,

plus la volonté existe de renforcer les droits, plus en même temps il est indispensable de renforcer aussi les devoirs ne serait-ce que pour garantir les premiers.

704. Une société de la protection risque alors d'être davantage bardée d'interdits, et même assez fortement liberticide. Cela vaut à tous les niveaux et à toutes les échelles.

705. En France, la cybercriminalité est prise juridiquement en compte depuis la loi *informatique et libertés* (loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978). Elle suscita d'ailleurs un certain nombre de critiques en son temps, mais présente au moins l'avantage de prendre pour la première fois en compte de nouvelles menaces. Elle fit ainsi preuve d'un certain esprit d'anticipation, même s'il n'est alors absolument pas possible de prévoir l'essor et le développement de l'informatique dans le futur.

706. Cette loi offre l'exemple d'une politique préventive. En l'absence de vues claires sur ce qui risque d'arriver, il semble important d'anticiper les choses, mais cela fait aussi courir la menace d'une prudence excessive et malheureuse ; qui pourrait tout paralyser et bloquer. Ceci étant, la loi de 1978 se présente, d'une certaine manière, comme un modèle du genre. Ainsi, elle stipule que les données collectées et traitées doivent l'être pour des finalités déterminées, explicites et légitimes. Elles ne doivent pas être traitées ultérieurement, de manière incompatible avec ces finalités. Les sanctions envisagées sont sévères.

707. Cette loi rassemble, par ailleurs, les droits des particuliers en quatre points : le droit d'information, le droit d'opposition, le droit d'accès et le droit de rectification. Ces droits ne peuvent pas être considérés isolément (l'un de l'autre), mais il convient néanmoins de les aborder l'un après l'autre. Le droit d'opposition, prévu à l'article 310 de ladite loi que toute personne a droit de savoir si elle est fichée ou non, dans quel fichier et de quelle façon. On peut dire que ce droit est, en quelque sorte, un socle pour d'autres. Le droit d'opposition autorise toute personne à s'opposer, pour un motif légitime, à ce qu'elle figure dans un fichier. De plus, elle peut s'opposer, sans justification, à ce que les données la concernant soient utilisées à des fins de prospection, en particulier commerciale. Cela concerne en particulier les fichiers du secteur privé.

708. Le droit d'accès est complémentaire du droit d'information, qu'il explicite d'une certaine façon. En effet, il permet, en justifiant de son identité, la consultation de ses propre données personnelles, afin de vérifier l'exactitude des données et d'obtenir une copie à très bas prix, au moins dans certaines limites.

709. Le droit de rectification complète les trois autres droits. Il permet de rectifier, compléter, actualiser, verrouiller ou faire effacer des données erronées la concernant. En voici la formulation par l'article 4012 : « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. »

710. La loi du 6 août 2004 qui transpose dans le droit français les dispositions de la directive 95/46/CE, apporte de nombreuses modifications à la loi Informatique et libertés. Elle a été complétée par des décrets pris le 20 octobre 2005 et le 25 mars 2007. Elle vise, en particulier, à harmoniser les règles de déclaration des fichiers entre secteur privé et secteur public.

711. Le régime général pour le secteur public n'est plus de demander une autorisation à la CNIL, mais de faire une simple déclaration de ces fichiers, comme c'était déjà le cas pour le secteur privé. Le demandeur doit alors attendre le récépissé de la CNIL avant l'utilisation effective du fichier. L'application qui est faite de ce changement de loi présente à l'époque quelques ratés en particulier lorsque le ministère de l'éducation nationale lance et utilise un des fichiers sans attendre le récépissé de la déclaration à la CNIL.

712. Par la suite, pour des raisons analogues, le Conseil d'État annula totalement le décret d'application de la base nationale des identifiants élèves, qui attribue un matricule à chaque enfant scolarisé dès l'âge de trois ans. L'Etat tend donc lui-même à ficher de façon irrégulière ou prématurée les citoyens. Ce qui est une lourde menace. Malgré cette volonté libéralisatrice du Conseil d'Etat Français, la distinction entre personne publique et personne privée n'est pas abolie. Les conditions sont toujours plus strictes pour le secteur privé. Ce dernier est soumis à une procédure d'autorisation pour un fichier ; surtout si ce dernier utilise des données de la sécurité sociale. La loi prévoit également la possibilité, pour un organisme privé ou public, de nommer un « correspondant à la protection des données à caractère personnel », couramment appelé « correspondant informatique et libertés » (CIL), qui a pour mission d'assurer l'application des dispositions de la loi à l'intérieur de l'organisme.

713. Le 25 janvier 2012, la Commission européenne a publié un projet de Règlement européen visant à remplacer la Directive 95/46/CE (et en conséquence à modifier en profondeur la loi Informatique et Libertés). Ce projet prévoit la désignation d'un Délégué à la protection des

données (évolution de la fonction de Correspondant Informatique et Libertés), qui serait obligatoire dans le cadre des autorités et organismes publics, et obligatoire au sein des entreprises employant 250 personnes ou plus, mais aussi dans les entreprises employant moins de 250 personnes (mais dont "les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées").

Pour situer le contexte de la loi et la difficulté de son application, il faut se souvenir qu'à la fin des années soixante-dix, Interpol décida d'informatiser sa base de renseignements, jusqu'alors encore traitée manuellement. Ce qui posa de nouveaux problèmes juridiques.

714. Un différend opposant Interpol (basée en ce temps-là à Saint-Cloud) à l'Etat français naquit. Ce dernier prétendit que sa loi s'applique aussi aux données contenues dans les locaux de l'organisation, locaux auxquels les autorités nationales françaises ont le droit d'accéder. Toutefois, Interpol estima que la loi ne s'appliquait pas. Ceci, pour deux raisons : d'une part, les informations contenues appartiennent en fait aux Etats membres. De même, Interpol n'en est que le gestionnaire. De sorte qu'elles bénéficient d'un statut d'extra-territorialité.

715. D'autre part, concrètement et pratiquement, soumettre les données sensibles ainsi détenues à la loi française serait - de fait - compromettre la coopération policière internationale. Certains pays préférant renoncer à communiquer des informations auxquels aurait accès librement l'État Français. Finalement, Interpol et l'Etat français se sont mis d'accord, le 3 novembre 1983, autour de deux principes forts : d'une part, celui de l'inviolabilité de fichiers et des archives d'Interpol ; d'autre part, celui de la nécessité de mettre en place une autorité de contrôle interne des fichiers ; et non pas nationale.

716. Le 5 février 1988, est adoptée la loi Jacques Godfrain, relative à la fraude informatique. Elle introduit les articles 323-1 et suivants dans le Code pénal, concernant notamment la suppression ou modification de données (art 323-1 al 1). Cette loi survint tandis que le *hacking* commence à exploser aux Etats Unis. Elle est peut-être en partie suscitée ou encouragée par un fait divers qui défraie alors la chronique. Le 28 novembre 1984, Le Canard Enchaîné publia un article détaillant la manière dont des journalistes ont eu accès à des bases de données, à l'aide d'un Minitel. Ceci, alors même qu'ils ne disposaient pas de connaissances techniques extraordinaires et n'ont pas eu recours à du matériel de grande qualité. Les données en question étaient pourtant d'une importance sensible – c'est le moins que l'on puisse dire, puisqu'il s'agit d'informations au sujet des essais nucléaires à Mururoa.

717. En 2004, la Loi pour la confiance dans l'économie numérique modifie la loi en ajoutant un article L. 323-3-1. Lequel réprime « le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 ».

718. Une affaire avait été largement diffusée dans le public. Elle focalisa l'attention sur des risques nouveaux. Il s'agit de l'affaire Damien Bancal[441], du nom d'un jeune journaliste français spécialiste des sujets de la délinquance informatique qui fut condamné pour avoir mis en évidence une faille sur le site d'une entreprise, sur son site Zataz.com. La Cour d'appel de Paris lui avait en effet reproché de semer un « trouble illicite ». Voici les faits. : Un lecteur du site signale à Damien Bancal que des documents confidentiels sont librement accessibles sur le serveur de l'entreprise *Forever living products*, spécialisée dans la production d'aloe vera.

    Cette entreprise, qui siège en Arizona, et qui pratique largement la vente directe, a simplement omis de sécuriser ses serveurs, rendant ainsi certaines informations accessibles à tous. Damien Bancal se contenta alors de signaler la faille qui existait. Ce qui bien entendu suscite l'émoi. Entre-temps, il prévient l'entreprise *Forever* qui colmate sa faille.

    Ce que la justice française reprocha en fait à Damien Bancal, c'est d'avoir publié un article détaillé décrivant l'origine du problème, en illustrant son article de captures d'écran qui prouve que le serveur informatique de l'entreprise était librement accessible.

719. En réalité, cette façon de faire est récurrente dans le milieu de la sécurité informatique. Une fois qu'une faille est décelée, elle est immédiatement signalée pour être colmatée au plus vite. Une fois que cela fut fait, et qu'il n'y avait plus de risque d'attaque, une brève note est publiée expliquant plus ou moins le problème, pour le bénéfice de l'ensemble de la communauté des internautes. Néanmoins, *Forever living products* se mit en colère. L'entreprise estima que la révélation de cette faille, même une fois colmatée, nuisait à son image (menaçait sa crédibilité). Elle assigna donc Damien Bancal en justice, au civil et au pénal, en l'accusant de s'être introduit illégalement dans son serveur et d'avoir diffamé l'entreprise. Même si l'intention diffamatoire ne fut pas retenue, le journaliste fut finalement condamné pour "trouble manifestement illicite". En effet, sa démarche d'investigation est somme toute assimilée à une action de piratage, même

[441] Qui est d'ailleurs l'auteur de deux ouvrages très intéressants sur la question : Damien BANCAL, *Hackers et pirates sur internet*, Strasbourg, Desmaret, coll. « Comportement » , 2001; *Hackers ! Le 5e pouvoir : Qui sont les pirates de l'Internet ?*, avec Yannick CHATELAIN et Loïc ROCHE, Paris, Maxima, 2001 ; « Le défacement, piratage en vogue », dans *Technologies internationales, ADIT,* 80, décembre 2001-janvier 2002, 33–36.

si son intention n'était pas celle des pirates habituels. En effet, le journaliste avait utilisé un moteur de recherche spécialisé. Il s'agissait, en fait, d'un instrument accessible à n'importe quel internaute un peu dégourdi. Ce jugement fit beaucoup d'encre. En effet, il constitua un revirement de la jurisprudence en vigueur, dite "jurisprudence Kitetoa". En effet, en 2002, le site Kitetoa, lui aussi spécialisé dans la sécurité informatique, avait été poursuivi par le groupe Tati, pour avoir révélé que le site de l'entreprise n'était pas sécurisé. Poursuivi, ce site de sécurité informatique, avait été par la suite relaxé, contrairement à Damien Bancal. Cette relaxe reposait en particulier sur l'argument selon lequel les internautes cesseraient de signaler aux responsables des sites les failles découvertes par hasard (par peur de poursuites judiciaires). De sorte que ces mêmes sites resteraient vulnérables et que de nombreuses attaques pourraient avoir lieu bien plus facilement.

720. Les deux décisions de justice ne sont donc pas harmonisées. Ce qui montrent bien que la question est délicate. Elle peut faire l'objet de différentes analyses. La décision à l'encontre de Damien Bancal pourrait traduire une évolution de la position dominante. Elle est peut-être également liée au profil controversé à l'époque de Bancal, quelquefois surnommé " l'ami des pirates ". Son attitude est souvent jugée ambiguë, par exemple, par le magazine électronique *Underground Cryptel*.

721. En 1999, déjà, Michel Meyer, alors Président Directeur Général de Multimania, avait qualifié les méthodes de Bancal d'illégales. Ainsi, des décisions de justice, au-delà des choix sur le fond, pourraient aussi s'expliquer, par le profil de telle ou telle personne incriminée, comme d'autres décisions de justice d'ailleurs.

722. La loi 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 », en son article 25 a complété la législation en vigueur. Elle a ajouté une exception, concernant le fait d'avoir « un motif légitime, notamment de recherche ou de sécurité informatique », d'effectuer les opérations en questions. La jurisprudence est donc complexe et certainement évolutive[442].

Ainsi, la lutte contre la cybercriminalité est en pleine évolution en France. Elle suscite de nombreuses discussions dans des sens les plus divers, selon les sensibilités des uns et des autres.

[442] Pierre-Alain WEILL, « Etat de la législation et tendances de la jurisprudence relatives à la protection des données personnelles en droit pénal français » *in Revue internationale de droit comparé*, 39, 3, 655-675. Cf. aussi Félix TREGUER, « Le droit pénal de la fraude informatique, nouvel ami des censeurs ? » *in La Revue des droirs de l'homme. Actualités Droits-Libertés*, 2 juin 2015*, https://halshs.archives-ouvertes.fr/halshs-01306609/*

Le plan de lutte contre la cybercriminalité, qui a été présenté en février 2008, contient des mesures visant à moderniser les méthodes d'investigation.

La même année, au mois d'octobre a été présenté le plan du numérique 2012 qui contient des propositions relatives à la lutte contre le cybercrime. Malgré cette évolution permanente, le dispositif législatif français en matière de cybercriminalité est « éparpillé » dans de nombreux textes. Il ne parvient pas toujours à laisser se dégager un position bien ajustée, y compris pour les juristes. Il n'est donc pas facile de déterminer de façon très précise, dans le droit français, ce qui relève - ou non - d'un acte cybercriminel.

723. Cela nous donne au moins deux enseignements précieux. Le premier, est que dans ce domaine, comme dans d'autres domaines (même si la gravité est assez marquée pour pouvoir justifier des recherches assidues), il n'est pas facile de trancher dans un sens, ou dans un autre[443]. Quelquefois, le lecteur a le sentiment d'évoluer dans un univers singulièrement complexe, avec un enchevêtrement considérable.

724. Le 23 novembre 2001, les pays membres du Conseil de l'Europe ainsi que les Etats-Unis, le Canada, le Japon et l'Afrique du Sud, adoptent une convention sur la cybercriminalité Elle se présente comme l'aboutissement d'un long processus de négociations et de recherches. Elle tente certainement de dégager une ligne médiane. Il s'agit d'une convention pénale, à vocation internationale, destinée à lutter contre le cybercrime. Néanmoins le sujet est complexe. En 2007, seuls quatorze États avaient ratifié la Convention, sur les quarante-sept signataires. Il faut signaler - au passage - que c'est en 2003 qu'a été ouvert - enfin - à la signature le protocole additionnel à la convention sur la cybercriminalité. Ceci, dans le souci d'élargir le champ d'application de la convention aux infractions de propagande raciste ou xénophobe, commis via les réseaux Internet. Ce protocole n'a pas été ratifié par les États-Unis. Notamment, car il inclut des éléments novateurs comme des mesures qui facilitent l'extradition et l'entraide judiciaire. Toujours est-il que la France a ratifié ces deux textes par la loi n° 2005-493 du 19 mai 2005, qui autorise l'approbation de la Convention du Conseil de l'Europe sur la cybercriminalité et du protocole additionnel à cette Convention. Les objectifs d'une telle convention sont clairement identifiables. D'une part, il est indispensable d'harmoniser les

[443] Myriam QUEMENER et Yves CHARPENEL, *Cybercriminalité. Droit pénal appliqu*é, Paris, .Pratique du droit, 2010. Myriam QUEMENER et Joël FERRY*, Cybercriminalité. Défi mondial*, Paris, Economica, 2 éd., 2009. Cf. aussi Myriam QUEMENER et Jean-Paul PINTE*, Cybersécurité des acteurs économiques : Risques, réponses stratégiques et juridiques,* Paris, Hermes Science Publications, coll. « Cyberconflits et cybercriminalité », 2012.

législations des Etats signataires après les avoir modernisées, y compris dans toutes les procédures engagées. Dans la mesure où les enjeux et les défis sont internationaux, il est important que la criminalité ne puisse profiter de la disparité nationale. La coopération internationale en matière d'extradition et d'entraide répressive semble particulièrement essentielle pour une vraie stratégie de lutte contre la cybercriminalité. Il est particulièrement important de donner partout – au moins pour l'essentiel – une définition semblable des infractions répertoriées par la Convention. Quatre séries d'infractions sont clairement posées. D'une part, les infractions informatiques, comme la falsification ou la fraude. En second lieu, les infractions de contenu, comme la pornographie enfantine. A cela, le protocole additionnel, qui ne recueille pas une égale unanimité, ajoute la diffusion d'idées racistes et xénophobes.

725. Le troisième type d'infraction sont celles liées à la propriété intellectuelle et aux droits connexes : comme le partage, au-delà du cercle familial et privé (qu'on évalue à environ dix personnes), des œuvres protégées.

726. Enfin, le quatrième type d'infractions regroupe les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes. Il s'agit de combattre l'accès illégal, mais aussi l'interception illégale, et l'atteinte à l'intégrité des données, ou des systèmes.

Un deuxième axe fort se distingue de la Convention. Il s'agit de mettre en place une cohérence procédurale, afin de définir les moyens d'enquêtes et de poursuites pénales les mieux adaptés à la mondialisation du réseau Internet. Ce qui s'avère singulièrement complexe.

727. La Convention prévoit des règles pour garantir les droits des individus, mais aussi pour faciliter la conduite d'enquêtes. Des règles sont spécifiées, comme celles qui préside à la conservation des données stockées, ainsi qu'à la conservation et à la divulgation des données relatives au trafic, à la perquisition des systèmes informatiques, ou encore à la saisie de données informatiques. Enfin, un troisième axe demande également toute notre attention. Il s'agit de la mise en place d'un système rapide et efficace de coopération internationale.

728. En plus des formes classiques - déjà bien reçues - de coopération pénale internationale, la Convention sur la cybercriminalité prévoit des formes d'entraide qui correspondent aux pouvoirs définis au préalable par la même Convention.

Elle vise donc à poser des bases solides et structurées, pour que les autorités judiciaires et les services de police d'un État membre puissent agir en coordination avec un autre État. De même, elle optimise la recherche de preuves électroniques ; en lui communiquant rapidement toutes les données et tous les résultats obtenus.

729. Il ne fait aucun doute pour personne que ce nouveau texte international, qui ne prétend évidemment pas répondre à toutes les questions ni résoudre tous les problèmes, constitue un complément indispensable aux législations nationales. Du reste, le 17 janvier 2005 le Conseil de l'Union européenne a adopté la Décision cadre 2005/222/JAI du Conseil relative aux attaques visant les systèmes d'information. Elle va permettre une harmonisation des règles pénales concernant les principales activités criminelles visant les systèmes d'information, l'atteinte à l'intégrité d'un système et l'atteinte à l'intégrité des données.

Les grands textes nationaux et internationaux, les décisions prises en amont, doivent bien entendu être relayés par des organes internationaux et nationaux de lutte, qui collent au plus près du terrain.

730. En France, par exemple, a été créé en 1998, le Département de lutte contre la cybercriminalité, au sein du service technique de recherches judiciaires et de documentation (STRJD, devenu SCRC) qui relève de la gendarmerie. Celle cellule est en mutation, en fonction du contexte et des besoins. Elle est - du reste - devenue la Division de lutte contre la cybercriminalité (DLCC), composée du Département coordination et appuis numériques (DCAN), du Département investigations sur Internet (D2I), du Département prévention et suivi des phénomènes sur Internet (DPSPI) et du Département répression des atteintes aux mineurs sur Internet (DRAMI), qui intègre le Centre national d'analyse des images de pédopornographie (CNAIP).

731. Toujours en France, c'est peu de temps après, le 15 mai 2000, qu'a été créé l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), au sein de la Direction centrale de la police judiciaire du Ministère de l'Intérieur. Cet office reprend la plate-forme de signalement des contenus illicites sur l'Internet. Toujours en l'an 2000, en complément de l'action de l'OCLCTIC, a été mise en place, la direction de la Surveillance du territoire (DST), qui est compétente pour diligenter des enquêtes judiciaires relatives à des actes de piratage sur les systèmes informatiques des établissements à régime restrictif ou des données classifiées de défense, singulièrement sensible comme chacun sait. Quelques années plus tard, en 2006 a été créé l'OCRVP, office central pour la répression des violences aux personnes, dont la mission est la coordination, sur le plan national, de la lutte contre les infractions violentes à l'encontre des personnes, notamment concernant la pédopornographie sur l'Internet.

732. Enfin, la police nationale français bénéficie aussi de services spéciaux, comme le SITT (Service de l'informatique et des traces technologiques). Les directions interrégionales et régionales de

police judiciaire ont à leur service des ICC (Investigateurs en CyberCriminalité), anciennement dénommés ESCI (Enquêteurs Spécialisés en Criminalité Informatique).

Qui plus est, elles peuvent également s'appuyer sur différentes brigades spécialisées, telle que la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI). Le 30 juin 2014, le magistrat Marc Robert présente son rapport à Bernard Cazeneuve, Axelle Lemaire, Arnaud Montebourg et Christiane Taubira, pour mettre en place des mesures juridiques et techniques visant à freiner les divers risques liés à la cybersécurité et améliorer la protection des internautes.

733. Parmi les mesures qui sont préconisées, il y a celles de la création d'un Centre d'Alerte, de l'ouverture d'un " 17 " de l'Internet ; ou encore de la mise en place d'une Délégation interministérielle à la lutte contre la cybercriminalité, placée sous la responsabilité directe du Premier Ministre.

Outre ces organes nationaux, il faut signaler le travail des organes internationaux, en particulier européens. Des compétences dans ce domaine ont alors été rapidement confiées à INTERPOL, dont le rôle est la facilitation d'échange de renseignements, afin de lutter efficacement contre toute forme de criminalité (notamment la criminalité informatique) De même, EUROPOL joue un rôle très important pour faciliter les échanges de renseignements entre les polices nationales européennes.

734. Il faut savoir que l'Union européenne (UE) a ainsi établi un Centre européen de lutte contre la cybercriminalité au sein d'Europol : EC3 (European Cybercrime Centre). Ce centre est chargé de soutenir les enquêtes des services spécialisés des États membres de l'UE, dans des domaines tels que toutes fraudes en ligne, comme celle à la carte de crédit. Il entend aussi éradiquer la pédopornographie et l'exploitation sexuelle des enfants en ligne (pédopornographie sur l'Internet). Il doit également empêcher toute cyberattaque contre les systèmes d'infrastructures sensibles de l'UE. L'EC3 prétend, de plus, offrir une contribution en matière d'analyse criminelle aux États-membres, en étant attentifs aux dernières tendances et aux inflexions.

735. EUROJUST, quant à lui, se présente comme un organe de l'Union européenne ayant pour vocation d'améliorer l'efficacité des autorités compétentes des États membres, dans la lutte contre la criminalité organisée transfrontalière, dont relève éminemment par sa nature même la cybercriminalité.

736. Enfin, depuis 2004 l'ENISA, Agence européenne désireuse de surveiller la sécurité des réseaux et de l'information, a différentes missions, dont celles de relever et d'analyser des données

relatives aux incidents liés à la sécurité, ou encore au suivi de l'élaboration des normes pour les produits et services en matière de sécurité de réseaux et de l'information. Cette agence se voue également à la promotion d'activités d'évaluation et de gestion des risques. A cela, s'ajoute encore, le programme européen Safer Internet destiné à lutter contre les contenus illicites, en vue d'un Internet plus *safe*.

Sur le papier, ces moyens juridiques et policiers de lutte contre la cybercriminalité font évidemment très forte impression[444]. Toutefois, sur le terrain, les choses se présentent comme un peu plus compliquées. Ainsi, il existe bien un certain nombre d'obstacles juridiques ou autres parfois, difficiles à prévoir en amont, auxquels on se heurte.

737. On pourrait mentionner, par exemple, le caractère très vaste des réseaux informatiques, ou la difficulté concrète à recueillir des preuves convaincantes, ou encore les limites délicates (et pas toujours précises) à ne pas franchir pour ne pas être accusé d'atteinte aux droits fondamentaux, comme le droit à l'anonymat ou à la liberté d'expression.

Comme nous n'avons eu de cesse de le souligner tout au fil de cette thèse, les décisions à prendre représentent souvent un point d'équilibre difficile à évaluer, entre des exigences contraires. Les visions éthiques et politiques des uns et des autres, et des différents pays, ne sont pas non plus les mêmes, il faut le savoir.

738. Cela est aussi lié au poids de l'histoire et à la " sédimentation des mentalités ". Une même conduite peut être considérée comme constituant une infraction dans tel ou tel pays et non pas dans tel autre. Cela est vrai, comme chacun le sait, de la consommation du cannabis, mais également des pratiques numériques.

739. Le principe de la territorialité de la loi pénale est bousculé. Par exemple, pour qu'un délit soit sanctionné en France, encore faudrait-il qu'il y en ait un élément constitutif sur ce territoire ? Ce n'est pas toujours le cas.

Il ne faut pas minimiser - non plus - le perfectionnement rapide des nouvelles techniques mises en œuvre par la cybercriminalité.[445] C'est un point important, que nous avons déjà souligné. Il ne touche pas seulement le domaine technique, mais juridique. En effet, légiférer dans un

[444] Mohamed CHAWSKI, *Combattre la cybercriminalité,* Perpignan, éditions de Saint-Amans, 2009.

[445] Cf. l'excellente thèse très pointue : Jean-Loup RICHET, *Complexité et dynamiques des stratégies d'influence lors d'une transformation organisationnelle liée aux systèmes d'information*, Nantes, 2017 : *http://www.theses.fr/s85185.* Aussi *:* Éric FREYSSINET, *La cybercriminalité en mouvement*, Cachan, Hermes Science Publications, coll. « Management et informatique », 2012.

domaine aussi délicat et sensible se fait bien entendu en prise directe avec les avancées pratiques.

740. Les nouvelles techniques de *hacking* sont de plus en plus faciles à mettre en œuvre et cela de plus en plus rapidement. Les conséquences requises pour devenir hacker sont de moins en moins difficiles à acquérir. Les coûts associés à une telle activité criminelle se présentent de façon de moins en moins rédhibitoire. Jamais encore les barrières à l'entrée n'avaient été aussi réduites. Quant aux services que l'on trouve facilement sur les plateformes, ils peuvent aisément être détournés, pour lancer des spams en très grand nombre, ou encore pour craquer un mot de passe, sinon augmenter la puissance d'un botnet. Il est de moins en moins difficile de devenir un cybercriminel. Pire encore, les communautés de *hackers black hat* commercialisent des logiciels qui donnent de se livrer à des attaques sans aucune compétence technique.

741. Des communautés en ligne de cybercriminels ne cessent de se multiplier ici et là. On trouve des kits pour devenir cybercriminel, clefs en main. La cybercriminalité risque donc de devenir un comportement de plus en plus fréquent[446]. Les banques[447] vont être certainement, elles aussi, de plus en plus menacées. Environ 80% de la cybercriminalité serait l'œuvre exclusive ou partagée de bandes organisées transfrontalières. Aux Etats-Unis, chaque année, la cybercriminalité occasionne une perte de 67 millions de dollars[448]. Dans le monde entier, cela peut s'élever à environ 400 milliards de dollars[449]. En France, on pense que chaque année plus de 26 millions de Français sont victimes de cybercrimes ; sans même parler des entreprises, qui vont être de plus en plus ciblées[450]. Comme le rappelle la police, nul n'est à l'abri[451]. Un roman décoiffant de science-fiction montre l'importance de l'enjeu et sa récurrence mieux vaut ne pas être chauve.[452]. L'enjeu est mondial. Le législateur ne peut se contenter de réfléchir et de statuer dans des espaces géographiques trop limités.

---

[446] Philippe BAUMARD, « La cybercriminalité comportamentale » in Revue française de criminologie et de droit pénal, novembre 2014 *: https://www.researchgate.net/publication/298417731_LA_CYBERCRIMINALITE_COMPORTEMENTALE_HISTORIQUE_ET_REGULATION*

[447] Myriam QUEMENER et Christian AGHROUM, *Etablissements financiers et cyberfraudes*, Paris, La Revue Banque, 2011

[448] Yves DROTHIER, « Le cybercrime à l'origine d'une perte de 67 milliards de dollars aux Etats-Unis » in Le Journal du Net, 24 janvier, 2006 : http://www.journaldunet.com/solutions/0601/060124_etudes-fbi-ibm-cyber-criminalite.shtml

[449] Audrey ŒILLET, « Le coût de la cybercriminalité évalué à plus de 400 milliards de dollars par an » : *https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/cybercriminalite/actualite-708391-cybercriminalite-coute-327-2013.html*

[450] Myriam QUEMENER, *Cybermenaces. Entreprises et internaute*s, Paris, Economica, 2008.

[451] Boris MANENTI, « Parole de cyberflic : 'nul n'est à l'abri d'une cyberattaque' » in *l'Obs,* 8 janvier 2020, 24. Cf. Pierre PENALBA et Abigaelle PENALBA*, Cybercrimes. Un flic 2.0 raconte*, Paris, Albin Michel, 2020.

[452] Elise FONTENAILLE, *Unica*, Paris, Stock, 2006.

b. Une culture mondiale de la cybersécurité

742. L'un des enjeux principaux des politiques à mener dans le monde entier, mais également dans les Emirats, est alors celui de cybersécurité[453]. Ce néologisme de plus en plus récurrent désigne une stratégie et son résultat, dans le sens d'une meilleure protection des personnes et des actifs informatiques matériels et immatériels. Les enjeux sont nombreux et multiples : économiques, stratégiques et politiques.

    En effet, les conséquences des cyberattaques s'étendent bien au-delà des systèmes d'information. Il s'agit d'aborder le problème et la perspective de la sécurité dans une perspective globale.

743. Cela demande à la fois une continuité politique et une vision à long terme. Il est à la fois nécessaire de trouver des parades du point de vue technique et de protéger des sociétés avec toutes leurs composantes et leurs dimensions. Et ce au niveau mondial. Des comparaisons ne manqueront d'ailleurs pas d'être faites entre les différents pays. Il existe même un Indice de la cybersécurité dans le monde (GCI), qui mesure le niveau de développement de chaque pays dans ce domaine. Il évalue l'engagement des pays en faveur de la cybersécurité au regard de cinq points essentiels (juridique, technique, organisation, prise de conscience et savoir-faire, coopération internationale).

744. Il est évident que tout doit aller très vite. Il est de toute première importance d'identifier rapidement les menaces, de se protéger, de détecter les attaques, d'y répondre, et de retrouver le plus vite possible un mode de fonctionnement normal. Il semble également hautement souhaitable de signaler de telles attaques. De même que l'on déclare la propagation d'une maladie infectieuse. Au-delà des affinements théoriques, l'approche doit être très opérationnelle. Ceci, afin de gérer rapidement des cyberattaques en temps réel, de réagir et de donner des ordres adaptés et pertinents.

---

[453] Nicolas ARPAGIAN, La Cybersécurité, Paris, PUF, coll. « Que sais-je ? », 2015 ; Ludovic PIETRE-CAMBACEDES et Yannick FOURASTIER*, Cybersecurite des installations industrielles : défendre ses systèmes numériques*, Toulouse, Éditions Cépaduès, 2015 ; Christian AGHROUM*, Les mots pour comprendre la cybersécurité : Et profiter sereinement d'Internet*, Paris, Lignes de Repères Editions, 2010.

745. Il s'agit donc bien de mettre sur pied, à différents niveaux, des I8SOC, en l'occurrence des *Information Security Operations Centers* pour mettre sur pieds et coordonner des politiques de cybersécurité, dans les organisations publiques et privées. De tels centres doivent contrôler l'ensemble des composants d'un système d'information, ainsi qu'être capable de détecter le plus rapidement possible des éléments caractéristiques d'une cyberattaque (avant d'adopter le plus intelligemment possible, c'est-à-dire aussi avec réalisme, la réaction des différents composants concernés dudit système d'information). Nous reparlerons plus loin de la cyberrésilience, qui est un dispositif complémentaire. En effet, une fois l'attaque conjurée, il s'agit de refaire fonctionner - dans les meilleures conditions possibles - le système. Ceci, afin qu'il reprenne son efficience, voire même qu'il en acquiert de nouvelles.

746. Depuis le Forum de Davos de 2018 dont nous reparlerons, il n'est plus satisfaisant de s'inscrire seulement dans une perspective défensive. Il convient encore de viser, en positif, une reconstruction, sinon une amélioration (car les épreuves enseignent toujours, et permettent d'aller plus loin avec plus d'énergie) du système. Comme le disait Nietzsche : " Ce qui ne nous tue pas, nous rend plus fort. "

747. Au-delà de la France, la législation souhaitable pour les Emirats s'oriente vers les choix qu'ont opéré, en la matière, les Etats Unis, exprimés par deux directives de la Maison-Blanche de 2013 et de 2015. Nous pouvons également noter la création, en février 2015, d'une nouvelle Agence dédiée à la cybersécurité, la CTIIC11.L'objectif caressé est bien entendu celui de protéger les infrastructures critiques des Etats-Unis, ainsi que de permettre à ce pays d'identifier les attaques et d'y répondre le plus rapidement possible (de façon coordonnée, en synergie), mais également de développer les partenariats internationaux et de responsabiliser les agences fédérales.

748. Sous la présidence de Barack Obama, les attaques se sont multipliées. Au début de l'année 2016, Barack Obama a renforcé les diverses initiatives, par l'annonce d'un plan d'action national en cybersécurité, dont le sigle est CNAP Il lui assigna pour principaux objectifs de protéger encore mieux la vie privée et la sécurité publique, mais aussi de poursuivre l'amélioration de la sécurisation économique dans le domaine, du numérique (tout en renforçant la sensibilisation et la protection de l'ensemble des parties prenantes, y compris au travers de l'augmentation du niveau sécurité informatique des agences fédérales).

749. Le budget associé est considérable, de l'ordre de 19 milliards de dollars US en 2017. Pour le nouveau Président Donald Trump, la cybersécurité constitue également une priorité. Avant

même son entrée en fonction, il avait déclaré vouloir mettre en place un comité d'experts pour renforcer les mesures et adresser les problématiques gouvernementales et privées dans ce domaine.

750. Le 2 novembre 2017, un projet de loi, baptisé SHIELD Act, a été annoncé pour renforcer la cybersécurité dans l'État de New York, particulièrement ciblé par les menaces. En juin 2019, en réaction à la destruction par l'Iran d'un drone américain, Donald Trump lance une cyberattaque contre les systèmes de lancement de missiles et un réseau d'espionnage iraniens. À présent, c'est la question de la protection de l'Internet des objets qui fait l'objet d'une enquête systématique.

751. L'Union européenne n'est pas en reste. Un projet de directive sur la sécurité des réseaux et des systèmes d'information du Parlement et du Conseil Européens est soumis à consultation au cours de l'année 2013. Il inclut, en particulier, des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union. Dans cette perspective, on pourrait imposer à certaines entreprises et à diverses organisations, un niveau de sécurité minimum pour les technologies, les réseaux et les services numériques dans l'ensemble des États membres. Il pourrait également leur appartenir de signaler les incidents de sécurité informatique majeurs dont elles sont victimes

752. En juillet 2016, le Parlement européen et le Conseil de l'Union européenne décident d'adopter une Directive sur la sécurité des réseaux et des systèmes d'information, connue sous l'appellation « directive NIS ». Cette dernière, prévoit le renforcement des capacités nationales de cybersécurité, ainsi que l'établissement d'un cadre de coopération volontaire entre États, tout comme le renforcement par chaque État de la cybersécurité d'opérateurs dits de services essentiels (OSE) au fonctionnement de l'économie et de la société.

    Elle mise, de façon très forte, sur l'instauration de Règles européennes communes en matière de cybersécurité des prestataires de services numériques (dans les domaines de l'informatique en nuage, des moteurs de recherche, ou encore des places de marché en ligne).

753. En France, c'est le 21 janvier 2014 que, pour la première fois, le Premier Ministre Jean-Marc Ayrault tint à souligner que la cybersécurité « est une question d'intérêt majeur et d'intérêt national qui concerne tous les citoyens, tous les Français, et c'est pourquoi il est important que le gouvernement s'engage totalement ». Son successeur, Manuel Valls, présente le 16 octobre 2015 cette Stratégie nationale pour la sécurité du numérique qui doit s'appuyer sur la formation et la coopération internationale. Il s'agit d'une stratégie d'ensemble assez sophistiquée qui

détermine les objectifs à atteindre et les orientations qui en découlent. Ceci, dans le but de conforter la sécurité et la défense de nos infrastructures critiques et d'accompagner la transition numérique (en définissant les différents leviers humains, techniques et opérationnels nécessaires à l'innovation). Elle est, également, sensée rassurer les Français. Sa dimension psychologique n'est pas négligeable.

754. Il faut noter, du reste, que l'article 15 de la Loi de programmation militaire pour 2014-2019 (votée en décembre 2013) détaille les obligations que le Premier ministre peut imposer aux Opérateurs d'importance vitale (OIV), en matière : de sécurisation de leur réseau, de qualification de leurs systèmes de détection, d'information sur les attaques qu'ils peuvent subir et de soumission à des contrôles. Des sanctions pénales sont bien entendu spécifiées pour le non -respect des obligations concernées.

755. La cybersécurité constitue en effet l'un des douze domaines du plan Vigipirate de lutte contre le terrorisme. Un label « France Cybersecurity »36, a de plus été mis en place pour sensibiliser les utilisateurs.

756. Le Royaume-Uni, quant à lui, a publié un plan stratégique 2016-2021 sur la cybersécurité, qui s'articule autour de trois objectifs. En premier lieu, il s'agissait de défendre le pays contre des menaces et d'y répondre efficacement, par différents biais. Dans un second temps, il fallait dissuader,par tous les moyens possibles et les plus rapide, de possibles attaques. Enfin, il convenait de développer et d'encourager un secteur d'activité autour de la cybersécurité.

757. Enfin, il peut être intéressant de s'intéresser aussi à ce qui se passe en Chine. Le 7 novembre 2016, le Congrès National du Peuple chinois adopta sa première loi fondamentale sur la Cybersécurité. Celle-ci suivit la consultation publique, en deux étapes, tenue en 2015. Cette loi définit, ainsi, la notion de "souveraineté nationale", dans le Cyberespace. Elle se fixa pour grands objectifs de maintenir la sécurité des réseaux informatiques et de protéger les données.

758. Cette loi donna un cadre juridique à l'exigence de sécurisation. A l'évidence, aucune des politiques nationales menées n'était exactement transposable dans un autre pays. En revanche, il est très utile et très fructueux de leur prêter attention et de les comparer, en se demandant comment les adapter à son propre pays.

759. C’est ce que sont en train de faire les Emirats Arabes Unis, avec la singularité qui est celle de leur histoire et de leur émergence tardive, mais également avec leur montée récente (plus ou moins au premier plan), à cause du pétrole et des prouesses d’une urbanisation intelligente et fort en pointe, notamment à Dubaï.

760. Il ne fait guère de doute que le marché de la cybersécurité, au Moyen-Orient et en Afrique, devrait connaître un taux de croissance annuel considérable. Ce qui invite à y placer des investissements innovants.

761. Dubaï reste en effet la ville phare en nouvelles technologies. Ceci, depuis que la perspective s’est ouverte de l’Exposition Universelle de 2020. Fixant cet horizon, on le sait, la ville s’est dotée d’infrastructures, de logiciels, d’outils toujours de plus en plus *high tech*. Bien entendu, cela renforce les risques d’attaques Internet, mais également (comme si d’un mal pouvait sortir un bien) peut doper tout le secteur de la sécurité. Il faut savoir que la cybercriminalité a touché plus de 3,72 millions de personnes en 2017. Il a engendré des pertes gigantesques. La nécessité de la combattre stimule un nouveau secteur d’activités, qui représente aujourd’hui plus de 25 Mds USD (et connaît une croissance supérieure à 11,8%).

762. Plus que tous les secteurs, celui de la cybersécurité s’avère porteur d’innovations. Du reste, par la création d’un « réseau de cybersécurité avancée » au service de 35 organismes fédéraux, les Emirats Arabes Unis se sont dotés d’outils, afin de contrer les attaques en ligne. Le Conseil de coopération du Golfe (CCEAG) devrait ainsi investir près de 11,4 Mds USD d’ici 2024. En septembre 2017, Cheikh Mohammed bin Rashid Al Maktoum, l’Emir de Dubaï et le Premier Ministre des Emirats Arabes Unis, ont lancé la Stratégie de Cybersécurité de Dubaï, articulée autour de 5 axes : Cybersécurité, Innovation, Collaboration nationale et internationale, Société cybersmart et Cyber résilience.

763. La Fédération des Banques des Emirats-Arabes-Unis (UBF) a, de plus, lancé en 2018 son premier Centre de partage et d’analyse de l’information. Tout ceci laisse entrevoir de belles possibilités pour les fournisseurs de solutions de cybersécurité spécialisées. Il faut souligner que la demande provenait aussi des sociétés privées émiraties, qui doivent se munir de systèmes de protection toujours plus performants (combinant systèmes DNS, protections DDoS, pare-feu, antivirus et autres systèmes de gestion des accès/authentification).

764. Il existe à Dubaï un Centre de cybersécurité Thalès, destiné sans doute à devenir dans la région un centre d'excellence en matière de services de conseil en cybersécurité. Il s’agit d’une réelle

opportunité pour le Moyen-Orient, en particulier pour les Emirats arabes unis, qui ne cultivent pas seulement d'énormes ambitions dans le domaine du numérique, mais disposent déjà d'infrastructures vraiment considérables. Très rapidement, la plupart d'entre elles, de plus en plus numérisées avec des technologies de pointe, sont vouées à s'appuyer sur l'expertise locale de Thales et à employer des méthodologies mondialement reconnues.

765. Le centre Thalès a également pour vocation de proposer des formations, des simulations et à fournir des renseignements sur les menaces. Il est évidemment primordial, grâce aux méthodologies utilisées dans ce Centre, de sensibiliser les entreprises de la région à la mise en œuvre de bonnes pratiques en matière de cybersécurité ; tout en développant, à cet effet, des partenariats avec des start-ups locales et des universités de renom.

766. Le niveau de sophistication des attaques suppose, en effet, un développement des recherches pour les parer, et un fort investissement. Les ripostes doivent non seulement être fortes, mais surtout très rapides. Dans ce but, il faut opérer de grands changements structurels. Et mieux coordonner aussi les prises de décision pour qu'elles soient immédiates. Il faut souligner que depuis trois ans Thalès a investi plus d'un milliard d'euros dans des technologies numériques clés, notamment l'IoT, le big data, l'intelligence artificielle et la cybersécuritéLe centre de cybersécurité de Dubaï pourra ainsi bénéficier d'une expertise technologique sophistiquée, des compétences acquises et de l'expérience du Groupe dans les systèmes critiques de sécurité.

767. Parmi les méthodes déjà utilisées, il faut évoquer : les bilans de santé en cybersécurité, la recherche de vulnérabilités, l'évaluation du risque spécifique aux systèmes ainsi que les formations, urgentes et prioritaires. Ces formations doivent être dispensées et suivies, en bénéficiant au maximum de l'expertise locale. Thalès s'emploie à valoriser l'avantage concurrentiel de ses clients. Celui-ci ne passe donc plus seulement par des technologies plus sophistiquées, mais par des stratégies de défenses moins vulnérables. Ainsi, il leur fournit des protocoles plus résistants et des opportunités de perfectionnement.

768. Pour reprendre l'analogie de la pandémie récente. Désormais, il ne s'agit plus tellement de parvenir à une prouesse en matière de nouveauté de produit, que d'exceller dans tout ce qui protège (par exemple le masque dans le cadre sanitaire). Les virus, biologiques ou numériques, placent désormais l'accent sur tout ce qui est défensive et non plus offensive, et le juriste se doit bien entendu d'en tenir compte.

769. Il importe en particulier d'exploiter les bonnes pratiques recueillies dans le cadre du programme STATION F, mis en place en 2017 en France par Thales, pour aider des PME expertes en

cybersécurité dans leur développement. Il est instructif de s'attacher aussi et encore à DarkMatter, une société de cybersécurité basée à Abou Dabi, qui a le vent en poupe. Des polémiques existent à son sujet. En effet, il semble que, dans un passé récent, le gouvernement émirati ait constitué 80 % de la clientèle de DarkMatter, souvent présentée comme un partenaire stratégique du gouvernement émirati. Toujours est-il que cette société offre toute une gamme - régulièrement élargie et de plus en plus sophistiquée - de services de cybersécurité non offensifs.

770. Darkmatters présente avant tout ses activités comme défensive, mais cela éveille des critiques et des soupçons d'une forme de volonté de contrôle universel. On prête quelquefois, dans la presse où ailleurs aux Emirat (mais cela vaut bien entendu aussi pour de nombreux autres pays), un usage perverti de la cyberdéfense et de la cybersécurité, dans un but tout autre en l'occurrence de développer un système de surveillance susceptible d'intercepter, de modifier ou de détourner le trafic sur les réseaux.

Le site The Intercept, par exemple, subodore de la part des Emirats une recherche agressive de hackers qualifiés pour procéder à des opérations de surveillance offensives, incluant des plans visant à exploiter les sondes de matériel informatique déjà installées dans les grandes villes afin d'exercer une activité occulte de suivi, de localisation et de piratage

771. À l'évidence, indépendamment de tout soupçon discutable concernant l'activité des Emirats, avancée dans le domaine de la cybersécurité peut en même temps inspirer de nouvelles techniques de cybercriminalité et aussi d'espionnage. Au-delà de toute polémique, il existe - sans aucun doute - un besoin en matière de cybersécurité aux Émirats-Arabes-Unis. On ne peut reprocher à ce pays de pousser loin la recherche pour se protéger. Même si indirectement cela peut conduire à des dérives. Depuis les soulèvements arabes de 2011, cependant, la « gouvernance interne de la cybersécurité », exploitée pour étouffer les signes avant-coureurs de révolte et réprimer les voix dissidentes, est devenue de plus en plus importante pour le gouvernement émirati et d'autres régimes de la région.

Ce souci s'est concrétisé dans la loi sur la cybercriminalité instituée en 2012. Celle-ci se voulut fortement répressive. Elle a été suivie de la formation de la propre entité des Émirats Arabes Unis en matière de cybersécurité, la *National Electronic Security Authority* (NESA). Cette dernière a récemment commencé à travailler en parallèle avec l'unité de cybercommandement des forces armées émiraties, créée en 2014.

772. Un réseau d'Agences gouvernementales émiraties et d'industries de télécommunication dirigées par l'État a travaillé en étroite coordination avec des fabricants d'armes internationaux et des sociétés de cybersécurité pour transformer les technologies de communication en éléments centraux d'un contrôle autoritaire. Plus récemment, en 2016, un responsable de la police de Dubaï a annoncé que les autorités surveillaient les utilisateurs de 42 réseaux sociaux ; tandis qu'un porte-parole de l'Autorité de régulation des télécommunications des Émirats Arabes Unis a également reconnu que tous les profils figurant sur les réseaux sociaux et les sites Internet étaient suivis par les agences concernées. Le New York Times, dans un article en date du dimanche 22 décembre a également accusé les services de renseignement d'avoir un accès direct aux messages et conversations vidéo échangées sur ToTok (ainsi qu'aux données de géolocalisation, à la liste de contacts, aux caméras, micros et calendriers du téléphone). Toujours selon le même journal, derrière l'application ToTok, lancée par Breej Holding, qui serait en réalité une société de façade de DarkMatter, se dissimulerait une activité de cyber-renseignement et de piratage liée au gouvernement émirati.

773. Elle serait l'œuvre de Pax AI. Il s'agit d'une société d'intelligence artificielle dont le siège est dans le même immeuble que l'agence d'écoute des Emirats arabes unis, à Abou Dhabi. Depuis, ToTok précise ne plus être disponible sur l'Apple Store et le Google Play Store pour des raisons techniques, même si l'AFP prétend que ce respect tient à un « problème de règles.» Du reste, Patrick Wardle, ancien hacker de l'agence d'espionnage américaine National Security Agency (NSA), interrogé par le Times, prétend que la spécificité de ToTok semblait résider dans le fait que l'application opérait en toute légitimité.

    En effet, les utilisateurs lui ouvraient eux-mêmes les portes de leurs contenus les plus personnels ; sans avoir conscience qu'ils étaient ensuite potentiellement exploités par un service de renseignement.

774. Tout cela semble vouloir dire que l'urgence de légiférer dans ce domaine, est évidente ;non seulement pour limiter les risques de dérives éventuelles de la part des Emirats, mais aussi pour éviter le soupçon à leur endroit, ou des accusations bien difficiles à vérifier, à infirmer ou à confirmer. Nous constatons à quel point il est important de bien délimiter les choses, les pratiques et les règles : non seulement, pour éviter des abus et des détournements toujours possibles, mais aussi et d'abord - sans doute - pour éviter un climat de suspicion qui détériorerait l'ambiance de la communauté internationale et empêcherait le minimum de confiance toujours indispensable.

Chapitre II : La cyberdéfense : Enjeu de civilisation et de survie.

775. Chaque individu, à juste titre, se soucie de sa sécurité individuelle. Au-delà de ce qui le concerne à titre personnel, il est forcément impliqué dans tout ce qui concerne le collectif, aux différentes échelles qui le constituent. Or, il se trouve justement que l'une de ces échelles - et non des moindres - est l'échelle nationale. C'est un pays tout entier qui peut être visé par des cyberattaques. Il peut être profondément déstabilisé par elle, avec une résonance, bien entendu, au niveau individuel. Mais c'est aussi une région ou un vaste espace comme l'Europe qui doit relever le défi. Il y a donc bien une sorte de véritable « guerre » qu'il s'agit alors de mener.

776. On pourrait parler de cyberdéfense. Le terme n'est pas d'un usage aussi simple que cela. Il faut préciser qu'il n'est pas exactement traduisible en anglais ou dans d'autres langues. En effet, souvent la défense est à entendre dans un sens limitatif de riposte à une attaque. De même que l'on oppose le défensif à l'offensif. Alors que le terme cyberdéfense a une acception bien plus large. Il désigne le cadre global de la conflictualité internationale liée au numérique ; incluant donc aussi des postures offensives.

777. La cyberdéfense est à la fois théorique et, on pourrait dire, opérationnelle. Le cyberespace international, déjà évoqué, inclut d'emblée une dimension stratégique (en lien avec un contexte global, lui-même mouvant). Il en va d'ailleurs du monde entier et de la civilisation. De la paix mondiale. Dans la mesure où il s'agit d'une conflictualité assez diffuse au demeurant. Elle fait peser de vrais risques de guerre.

    Il faut donc se soucier aussi bien du *ius in bello* que du *ius ad bellum* : à savoir, de ce qui est acceptable (ou non) dans le conflit, et s'il est acceptable (ou non) d'entrer en guerre. Bien entendu, le type d'interrogation dans les deux sortes de droit est articulé. Il renvoie aux mêmes enjeux fondamentaux de conservation pour assurer sa sécurité, celle des autres et des bien. De même, il contribue à l'évaluation du risque.

778. Les questions les plus classiques concernant le droit de la guerre[454] remontent à la surface, mais dans un autre contexte. Ou plutôt analogue : à savoir le même pour certaines interrogations fondamentales et différent pour le contexte, et parfois l'ampleur ou la sidérante rapidité de ce qui peut survenir.

[454] David CUMIN, *Manuel de droit de la guerre*, Bruxelles, Larcier/Bruylant, 2014.

779. En 1993, David Arquilla et John Ronfeldt lancent le terme « cyberguerre »[455]. Ils entendent faire prendre conscience des effets des technologies numériques sur le déroulement des conflits futurs. Ils sont - du reste - convaincus que c'est souvent l'obtention des meilleures informations qui fait les vainqueurs. D'où l'importance d'ailleurs des services de renseignements, en temps de paix et surtout en temps de guerre. Rien de neuf sous le soleil : Fouché sous Napoléon, ou Hoover aux Etats-Unis jadis, en étaient déjà convaincus.

Toutefois, cette exigence prend une ampleur nouvelle. Le renseignement est plus facile à obtenir que jadis. Sa collecte comme sa gestion peuvent être très systématiques. Parfois, trop d'informations mal évaluées, mal vérifiées et surtout mal articulées peuvent brouiller le discernement, et rendre plus pesante l'action à adopter.

780. Ainsi, l'inscription réciproque du numérique dans la conflictualité, et de la conflictualité dans le numérique, ne semble pas aussi évidente que cela[456]. La guerre se caractérise par des critères de violence, que l'on ne retrouve pas toujours dans les cyberattaques (dont la nature exacte et l'évaluation ne sont pas forcément évidentes).

Par exemple, les cas d'effets létaux ou physiques, ou même de dommages physiques sur les infrastructures dans le cas d'attaques numériques demeurent assez rares. À l'exception sans doute du virus Stuxnet contre les centrifugeuses d'enrichissement de d'uranium de l'usine iranienne de Natanz en 2014, ou depuis les attaques contre le système de distribution électrique de l'Ukraine.

781. Il est également vrai que nous sommes au carrefour de la guerre. En particulier avec les trois catégories qui englobent les attaques numériques : le sabotage, l'espionnage et la subversion[457]. Nous sommes donc, au-delà des querelles de vocabulaire, face à un phénomène nouveau qu'il est impossible d'éluder. Dont il faut prendre conscience de l'importance et de la dangerosité. Le défi est considérable. Il nous importe de le relever, pour conjurer le grand danger d'une très graves perturbation internationale[458].

Pour mieux situer les enjeux de la cyberdéfense, il est intéressant d'inventorier les vulnérabilités qui conditionnent les attaques, et, d'une certaine manière, les appellent. Cette question des vulnérabilités concerne aussi la cybercriminalité du quotidien, qui s'en prend à des particuliers.

---

[455] John ARQUILLA et David RONFELDT, « Cyberwar is Coming » in *Comparative Strategy*, 12, 2.
[456] Ben BUCHANAN et Thomas RID, « Attributing Cyber Attacks » in *Journal of Strategic Studies*, 38, 1-2, 4-37.
[457] Thomas RID, « Cyber War Will Not Take Place » in *Journal of Strategic Studies*, 35, 1 (-32.
[458] Lucas KELLO*, The Virtual Weapon and International Order,* New Haven, Yale University Press, 2017.

Dans une guerre classique, il s'agit bien entendu d'évaluer la vulnérabilité de l'adversaire. Ce que l'on peut appeler ses points faibles. Sans minimiser ses capacités de résistance, ses protections, ses ripostes défensives.

782. Il en va de même *mutatis mutandis* de la guerre dans l'espace numérique. C'est la géopolitique qui permet de comprendre le cyberespace[459], qui n'a rien d'une simple usine à gaz purement technique. De même, les attaques sont menées en raison des vulnérabilités, plus ou moins importantes. Certaines sont plus difficiles à détecter et certaines plus visibles. Souvent, la vulnérabilité tient à la facilité d'accès : par n'importe quel point du réseau ou au contraire par un accès au réseau local. L'un des problèmes spécifiques et récurrents d'une cyberattaque tient à la difficulté d'identifier celui qui l'a lancée, en l'occurrence à l'attribution[460]. Les technologies permettent de dissimuler le fait d'être à l'origine d'une telle action.

783. Cette difficulté donne un avantage même temporaire à l'agresseur. En effet, le temps d'enquête (l'hésitation dans la détermination d'une responsabilité) le rend quelques temps maître de la situation. De sorte que l'on peut estimer que dans la cyberdéfense c'est l'attaquant qui se trouve en posture plus favorable.

Cela se confirme, dans la mesure où un doute peut longtemps planer, et que des preuves irréfutables sont très difficiles à rassembler. Or, pour préserver la paix et l'ordre international, il est très dangereux de pointer du doigt un responsable non véritablement avéré d'une attaque.

784. Du reste, cela représente une véritable offense de tous les principes du droit international et un viol d'une sorte de présomption d'innocence d'un genre particulier. Le fait que toute recherche du coupable d'une cyberattaque demande beaucoup de temps est d'autant plus handicapante que, dans le cadre de la cyberdéfense, beaucoup tient à la rapidité de l'esquive, de la parade, de la riposte.

785. La victime hésite à s'en prendre à un agresseur possible ou probable. Il y a, en effet, un grand risque d'escalade, non seulement si l'attaquant présumé est innocent. Même s'il est en définitive coupable, mais s'en défend, il n'y a de vraies preuves. Du reste, même dans le cas de vraies preuves, elles peuvent être mises en cause et présentées comme fabriquées, dans un cadre où l'habileté de la communication et une rhétorique impavide l'emportent sur une démonstration, du reste improbable. Si la victime d'une attaque s'abstient de désigner un coupable, elle est

[459] Frédérick DOUZET, « La géopolitique pour comprendre le cyberespace » in *Hérodot*e, 2014, 1, 7-13.
[460] Stéphane TAILLAT, « Le cyberespace et la conflictualité internationale » in collectif, *La cyberdéfense (op. cit.),* 26-34.

également perdante. En effet, elle perd son crédit et toute position de force. En réalité, un peu comme au jeu d'échec, tout dépendra du positionnement stratégique de l'un et de l'autre.

Plus encore que dans les situations de conflit classiques, les technologies et le domaine numérique nous conduisent dans une zone de turbulences et d'incertitude[461] à tous égards qui est redoutable déjà par ce fait même indépendamment de ce qui advient ensuite et de ses conséquences. Un tel climat d'incertitude ne peut que créer un surcroît de très vive tension. Et certainement aussi de risques.

786. Une certaine confusion peut demeurer sur les intentions des uns et des autres, autour de la pénétration des autres réseaux, dans un but offensif ou préventif. Ce qui contribue à une grande instabilité et quelquefois à un piétinement par indécision.

787. Deux raisons favorisent principalement les risques d'escalade. D'une part, l'asymétrie entre deux puissances hostiles. D'autre part, l'absence de régime stratégique marqué. Cela veut dire qu'en cas de conflit, les enjeux ne sont pas les mêmes entre les partenaires, notamment entre l'Europe et les Etats-Unis d'un côté, et la Russie ou la Chine de l'autre. Comme le note justement Stéphane Taillat : « Pour les premiers, le cyberespace est avant tout un domaine technique caractérisé par les risques que posent les attaques sur les infrastructures permettant le fonctionnement des activités financières, économiques et sociétales. Pour les seconds, le cyberespace est une partie de la sphère informationnelle et les principales menaces pèsent sur la stabilité politique et sociale des régimes et des sociétés qu'ils organisent »[462]. Pour certains pays, plutôt que pour d'autres, les avancées numériques se présentent donc comme un moyen d'intimidation et de désinformation.

788. Les jeux stratégiques des uns et des autres ne sont donc pas équivalents. Ils ne se déploient pas de la même façon. La stratégie des uns et des autres n'étant pas identique, ni du reste constante, il devient quelquefois difficile pour les uns et pour les autres de se situer et d'essayer d'identifier la stratégie des autres.

789. Certains pays comme la Russie s'inscrivent plutôt dans une logique de compensation par rapport à une puissance hégémonique comme les Etats-Unis. Une certaine obscurité d'ensemble

[461] Ben BUCHANAN, *The Cybersecurity Dilemma : Hacking, Trust and Fear Between Nations*, Londres, Hurst&Co, 2016.
[462] Stéphane TAILLAT*, Ibid.,* 30.

règne ; dissimulant des intentions cachées, mais aussi peut-être des fluctuations de positionnement très dérangeantes pour penser une défense[463].

Ce climat d'incertitude rend - en tous les cas - beaucoup plus complexe quelque consensus que ce soit au niveau international. Par exemple, sur la définition de la cybercriminalité ou du cyberterrorisme, sur des accords contraignants, sur la définition d'une véritable attaque numérique et plus encore sans doute sur le droit ou non à la légitime défense.

790. Il semble donc devenu de plus en plus difficile d'émettre des normes et des règles applicables à tous et acceptées par eux[464]. Se dissipe hélas de plus en plus la vision d'un cyberespace comme un espace positif et constructif d'échange et d'avancées communes.

Ceci, au profit d'une réalité somme toute menaçante. Où il y aurait plus à perdre qu'à gagner, et où l'essentiel serait précisément de parer une attaque difficile à prévoir. Dit plus simplement, de piéger l'autre avant d'être piégé par lui. Selon certains, cela serait singulièrement vrai depuis que la Chine exerce une si forte influence. Il s'agit certainement d'un climat assez largement partagé par ailleurs[465].

L'un des phénomènes observés, qui peut aussi être contesté ou nuancé, est celui de l'intrication d'acteurs non étatiques dans une conflictualité qui touche pourtant directement les Etats.

Cela peut se faire par le biais de logiciels malveillants, comme les malwares, ou par l'entremise de hackers. La survenue de ces nouveaux acteurs sur la scène internationale crée sans doute un effet notable de perturbation[466]. La suprématie des acteurs étatiques est donc mise en cause.

791. L'exploitation et la maintenance de beaucoup de réseaux relevant désormais d'agents privés, la contribution de ce secteur privé devient donc de plus en plus opportune et forte. Notons au passage que cela peut renforcer la difficulté de l'attribution, déjà évoquée au préalable. On peut quelquefois parler de recours à des mercenaires[467].

Même si elle est évaluée de façon très différente, il y a bel et bien une sorte de convergence entre les sphères étatiques et les secteurs privés ; parfois même - mais pas toujours - les moins recommandables. Cette convergence est cependant tout sauf simple. L'autonomisation

---

[463] Alexander KLIMBURG, *The Darkening Web : The War for Cyberspace*, Londres, Penguin Press, 2017.
[464] Alex GRISBY, « The End of Cyber Norms » in *Survival,* 59, 6, 109-122.
[465] Jon LINDSAY, « The Impact of China on Cybersecurity : Fictions and Frictions », in *International Security*, 39, 3, 7-47.
[466] James ROSENAU, *Turbulence in World Politics. A Theory of Change and Continuity*, Princeton, Princeton University Press, 1990.
[467] Tim MAURER, *Cyber Mercenaries : the State, Hackers and Power,* Cambridge, Cambridge University Press, 2018.

d'acteurs non étatiques avec leur logique propre perturbe le jeu, un peu comme un chien dans un jeu de quilles.

792. Ce facteur supplémentaire d'incertitude et d'instabilité tend plutôt à rendre l'atmosphère plus orageuse et menaçante encore. Paradoxalement, ce contexte incertain et menaçant pousse les Etats à réaffirmer leur influence, sinon leur contrôle et leur pouvoir sur le cyberespace. D'ailleurs, ils peuvent quelquefois tirer les ficelles, en laissant croire que l'initiative viendrait d'agents non étatiques, voire de rebelles.

793. On peut émettre l'hypothèse d'un retour des gouvernements dans le champ international, paradoxalement, par le biais d'un cyberespace. Ce dernier, semble induire - et en réalité induit bien au départ - le contraire d'un tel retour. Cela serait singulièrement vrai de la Russie[468]. En tous les cas, les Etats ont progressivement mis en place des structures et des doctrines de cyberdéfense pour développer des capacités offensives et défensives au profit de leurs forces armées.

794. Cela a été très clair lors des opérations menées par les Etats-Unis en Irak, en Afghanistan ou en Syrie. Comment passer sous silence l'appui fourni par les hackers aux forces russes et séparatistes en Ukraine. Néanmoins, comme toujours en définitive, dans les conflits et les guerres, il n'est pas du tout suffisant de s'intéresser aux aspects techniques. Encore faut-il les situer dans un contexte toujours unique, complexe et mouvant. Néanmoins, plusieurs précisions peuvent - et doivent - cependant être faites sur les aspects juridiques et stratégiques de la cyberdéfense. Elles peuvent ensuite orienter des mesures à prendre à différents niveaux et à différentes échelles (souvent provisoires du reste, du fait de l'évolution des techniques, des contextes et des enjeux).

[468] Kévin LIMONIER et Maxime AUDINET, « La stratégie d'influence informationnelle et numérique de la Russie en Europe » in *Hérodote*, 2017, 1, 164, 123-144.

***Section* I *: Les aspects juridiques et stratégiques de la cyberdéfense*[469].**

795. Souvent, le point de départ de toute avancée juridique ou stratégique est une contrariété, une attaque ou un problème. C'est également le cas en matière de cyberdéfense. De fait, depuis plusieurs années, on assiste à une multiplication d'actes malveillants pour des raisons et dans des cadres divers. Les attaques contre l'Estonie en 2007, mais aussi Stuxneten 2011, marquent sans doute un tournant.

796. La question est alors celle de l'application et déjà de l'applicabilité du droit international au cyberespace. En 2013, les Etats réunis au sein du Groupe d'experts gouvernementaux (GGE) en charge de la question estimèrent que le droit international pouvait et devait s'y appliquer. À partir de ce beau principe, il n'est cependant pas aisé de poser les détails.

797. Les Etats ne sont pas tous d'accord sur la ligne à adopter en la matière. Certains, souhaitent des engagements politiques ponctuels et audacieux :non pour poser de nouvelles obligations strictes, mais plutôt pour mieux cerner les activités des Etats, et ensuite mieux les évaluer. D'autres, en revanche, cultivent une approche légaliste, qui passe par de nouvelles obligations consensuellement reconnues. Ce qui semble plus compliqué à acquérir. Leur conviction est cependant faite. Le droit international existant n'est pas assez précis et adapté, pour bien réguler les conduites dans le cadre d'un cyberespace qui modifie beaucoup de choses et pose des problèmes nouveaux.

Toutefois, la question se pose de façon très complexe - et en partie paradoxale. En effet, d'un autre côté, les réalités du cyberespace sont parfois perçues comme justifiant une remise en cause de l'applicabilité de pans entiers du droit international.

Ainsi, loin de contribuer à faire plus de droit, la conflictualité numérique sèmerait le trouble et conduirait plutôt à mettre en cause la fiabilité du droit existant, au moins en partie. Le point de départ d'une telle remise en cause critique est le fait incontestable, déjà souligné, d'une grande difficulté à attribuer techniquement une attaque informatique à un Etat particulier.

Les possibilités de contournement, ou de dissimulation, deviennent désormais trop nombreuses. Cette impossibilité (ou du moins cette extrême difficulté) est, bien entendu, lourde de conséquences. En effet, sans attribution technique, il est impossible de recourir aux contre-

[469] François DELERUE et Aude GERY, « le droit international et la cyberdéfense », in collectif, La cyberdéfense (op.cit), 61-70.

mesures et a fortiori à la légitime défense qui supposent une claire identification du responsable, sans quoi c'est la porte ouverte à toutes les escalades.

798. Sur d'autres besoins aussi, il y a une contestation de la portée du droit international, et de sa pertinence dans le cadre de la cyberconflictualité. C'est, en partie, le cas à cause de spécificités essentielles du nouveau cadre du cyberespace ; qui empêche la transposition d'un autre cadre plus classique.

Par exemple, le seuil de distinction entre recours à la force et agression armée devient flou et cesse donc d'être opérationnel. Ce constat pourrait alors conduire à une acception plus large de la notion d'agression armée. Ce qui rendrait le contexte encore plus orageux et menaçant, d'autant que dans ce cas le recours à la légitime défense serait nettement facilité.

799. Il faut également rappeler que peu d'Etats ont recours au droit international lorsqu'il s'agit de trouver une solution à un problème posé par un autre Etat dans le cadre du cyberespace, en raison de la complexité du discernement juridique à opérer. La Cour internationale de justice n'a pour l'instant été saisie d'aucune affaire relative à un comportement agressif dans l'espace numérique, ce qui en dit long.

a. Licéité des cyber-opérations

800. Les considérations qui précèdent nous laissent deviner combien il est difficile de se prononcer en faveur (ou non) de la licéité des cyber opérations en général ; et de telle ou telle cyber opération en particulier. D'emblée, on peut se demander si la grande majorité des cyber opérations conduites pour le compte des États (peu importe en définitive que cela soit par le biais de forces armées ou d'autres agents) n'échapperaient pas - en fait - au droit des conflits armés[470] et ne relèveraient pas, en fait, d'autres branches du droit, qu'il resterait alors à expliciter. Toutefois, à supposer même que cela soit le cas, on pourrait envisager les cas, même rares, où le droit des conflits armés pourrait rester applicable.

801. Deux cas semblent envisageables. Le premier, est celui d'opérations intervenant dans le cadre d'un conflit déclaré. Les cyber opérations ne constitueraient qu'un élément ajouté. On peut penser à cet égard aux cyber opérations, qui ont en effet eu lieu dans le cadre de conflits armés existants (en Géorgie, en 2008, en Libye en 2011, ou encore en Syrie la même année). Le

[470] Michael N. SCHMITT et Liis VIHUL (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2éd., Cambridge, Cambridge University Press, 2017.

second, serait celui où ces cyber opérations constituaient en elles-mêmes un nouveau conflit armé, on pourrait dire *sui generis*. En théorie cela est bien entendu envisageable, mais pour le moment aucun exemple d'histoire contemporaine toute récente ne peut en être donné. On peut même conjecturer qu'il est assez peu probable qu'un conflit circonscrit à l'espace numérique puisse en fait être déclaré cyber conflit armé.

802. Les définitions n'ont pas véritablement la rigueur d'une formule mathématique. En ce domaine, la plus grande rigueur semble de mise. D'un point de vue pragmatique, il ne fait cette fois aucun doute que des cyberattaques (plus réduites) et des cyber opérations (plus larges) peuvent en effet offrir un moyen très efficace et parfois décisif d'intervention. Même s'il semble difficile de penser qu'on puisse contrôler entièrement tout un territoire seulement par le numérique.

803. Un Etat tiers pourrait cependant conduire des opérations de soutien à un belligérant, de même qu'un groupe non étatique pourrait, lui, soutenir un tel belligérant par des actions numériques. Il est légitime de penser, du reste, que de telles opérations dans le cadre d'un conflit déjà ouvert pourraient en modifier la nature. Favorisant, par exemple, son internationalisation.

804. La question évidemment essentielle est celle de la possibilité d'un point de vue juridique de recourir à la force. Ce qui porte également l'accent, bien entendu, sur l'interdiction juridique du recours à la force par le droit[471]. Cette question suppose de déterminer clairement qui est l'État responsable, et qui est l'Etat victime. Ce qui paraît plus embrouillé et improbable dans le contexte d'une guerre numérique. Il semble difficile de nier, dans l'abstrait, la licéité pour un État de mener certaines cyber opérations pour que certaines conditions soient effectivement réunies et vérifiées.

Toutefois, le principe général, une fois de plus, ne donne pas une solution à tous les problèmes concrets. Exprimé autrement, il n'existe donc pas d'interdiction générale et absolue de cyber opérations. Ce qui n'implique évidemment pas que toute cyberopération soit légitime. Leurs effets, par exemple disproportionnés, peuvent en effet les rendre illégitimes. Mais une cyber opération peut également être jugée illégitime, parce qu'elle violerait la souveraineté territoriale d'un Etat, ou qu'elle interviendrait dans les affaires de cet Etat.

805. Il y aurait violation de la souveraineté d'un Etat en fonction de deux critères cumulatifs. D'une part, il faudrait qu'il s'agisse d'une action menée par un État contre un autre État, directement

[471] Olivier CORTEN , *Le droit contre la guerre : l'interdiction du recours à la force en droit international contemporain*, Paris, Pedone, 2014.

ou plus souvent encore par des mercenaires. D'autre part, il est également indispensable que la cyber opération concernée agisse sur des systèmes informatiques situés sur le territoire ou sous la juridiction de l'Etat concerné.

Ces précisions semblent intéressantes. En effet, dans les faits, les intrusions d'un Etat dans un autre État semble se multiplier. Par exemple, pour saboter un processus électoral. Ce qui est parfois reproché à la Russie[472].

806. On peut dire qu'une intervention illicite pourrait se caractériser par deux éléments. Primo, il s'agit d'une opération d'un Etat contre un autre Etat. Secundo, l'objectif de cette opération est de contraindre l'Etat concerné à modifier sa conduite et ses choix dans ce qui relève de sa propre souveraineté. A cet égard, Stuxnet, dont nous avons déjà parlé offre un bon exemple d'une opération illégitime de ce type.

On le sait, c'est l'adoption de la Charte des Nations Unies en 1945, à l'issue de la Seconde Guerre mondiale, qui marque un grand tournant. Elle dénonce et interdit le recours à la menace ou à la force. A l'époque, les cyber opérations n'existaient pas. Cependant, on peut dire que cette interdiction s'applique pourtant à nombre d'entre elles.

807. Au-delà d'un critère qualitatif et formel, on pourrait envisager encore un critère d'intensité. Il reste, il est vrai, encore sujet à débat. Une cyber opération qui causerait trop de dégâts physiques ou même numériques pourquoi pas ; *a fortiori* qui causerait des blessures à des humains ou leur mort, ou d'importants ravages psychologiques, pourrait être considérée comme un recours abusif et illicite à la force (équivalent à une attaque armée).

808. Nous vivons dans un monde un monde très sensible à l'exigence de dédommagement des victimes, de réparation à leur endroit. Ce qui est un aspect parfois contestable, sans doute, mais dont les mesures législatives se doivent de tenir compte. Le droit semble désormais investi d'une fonction compensatrice ou réparatrice à l'égard de victimes innocentes qui semble orienter différemment, aujourd'hui, certains choix faits ou à faire.

809. Dans le mesure où l'on pourrait reconnaître au recours à la force de l'attaquant une grande gravité, il semble que cela pourrait ouvrir le droit à l'Etat victime d'engager une riposte dans le cadre de la légitime défense.

[472] Nicolas VANDERBIEST, « Les institutions démocratiques : l'influence des réseaux sociaux durant une élection présidentielle » in collectif, *La cyberdéfense, (op. cit)* 181-188.

Ce qui impliquerait aussi que, si le recours à la force dénoncé n'atteignait cependant pas le niveau de gravité requis, il ne serait alors pas possible d'entrer dans le cadre de la légitime défense. À l'évidence, le problème est de savoir comment mesurer cette légitime défense et selon quels critères.

810. Concrètement, il semblerait que seule la cyber opération du virus Stuxnet, menée nous l'avons dit par les Etats-Unis et Israël contre l'Iran, puisse véritablement être considérée pour le moment comme déployant un emploi illicite de la force de façon assez grave pour constituer une sorte d'attaque armée justifiant la légitime défense. Toutefois, cela ne veut pas dire que dans des cas moins extrêmes, il ne puisse y avoir d'autres réponses possibles, d'autres mesures de riposte en cas de cyber opération. Ceci, même si elles ne relèvent pas du droit de légitime défense et du recours à la violence légitime. Il s'agit, en l'occurrence, de contre-mesures proportionnées.

Il pourrait s'agir en l'occurrence de mesures de rétorsion inamicales, certes, mais en soi nullement illégales, ou même de mesures ordinairement illicites ; à savoir, comme des actes pris par un Etat en réaction à un acte gravement illicite d'un autre. Le caractère de contre-mesure rend licite ce qui est habituellement illicite.

811. C'est seulement lorsqu'une cyber opération est assez grave pour être assimilée à une agression armée que l'Etat peut invoquer son droit à la légitime défense, pour avoir véritablement recours à la force. Ce qui ne signifie aucunement qu'il n'y ait pas moyen de riposter dans des cas d'opérations moins graves ; mais de façon proportionnée, et mineure si l'on ose dire.

Dans la mesure où l'on peut estimer que dans un futur proche les cyber opérations prendront un autre ampleur, il semble opportun d'approfondir des critères permettant de reconnaître dans une cyber opération un attaque grave assimilée à une attaque armée[473].

b. Dissuasion et coercition[474]

[473] : Karine BANNELIER-KRISTAKIS, « Cyber Diligence : A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations ? » in *Baltic Yearbook of International Law*, 2015, 14, 1, 23-39.
[474] Stéphane TAILLAT, « Dissuasion et coercition » in *La cyberdéfense*, (op.cit), 141-149.

812. Face à des menaces, le souci évident et premier est de les éviter, et d'éviter en particulier l'escalade. La dissuasion[475] relève de la défense, en l'occurrence préventive. La coercition en revanche paraît davantage relever de l'offensive mais dans un même but préventif.

La dissuasion empêche qu'un mal se produise. La coercition relève d'une action accomplie pour forcer l'autre. La dissuasion s'adresse à la liberté et la coercition davantage qu'à la contrainte.

La dissuasion est forte. Elle se développe lorsque les menaces sont conséquentes et que les armes ou les conséquences peuvent légitimement faire très peur. Ce qui est le cas avec le péril d'une guerre nucléaire. Bien entendu le contexte de son émergence et de son développement est celui de la guerre froide.

Il y a une anticipation du risque qui conduit l'agent à faire machine arrière, et à se montrer plus complaisant. Le ressort psychologique est donc de première importance. On le sait, la dissuasion a surtout acquis ses lettres de noblesse, dans le cadre de la guerre froide. Elle consiste, en définitive, à influencer le comportement d'un acteur de sorte qu'il s'abstienne de faire quelque chose.

813. On peut dire que la dissuasion opère en général de deux façons. D'une part, en faisant miroiter des représailles. On peut parler d'un effet psychologique bien précis qui est la crainte d'une maximalisation des coûts pour celui qui agirait de sorte qu'il renonce à lui-même à ce qu'il n'a pas intérêt à faire.

La dissuasion semble, en effet, supposer une sorte de rationalité dans les choix. De sorte que le plus astucieux est de faire qu'une personne physique ou morale renonce d'elle-même à ce qui n'est pas son intérêt. Il s'agit en quelque sorte d'une variante du scénario «gagnant / gagnant », que l'on pourrait définir « non perdant / non perdant ». D'autre part, une forme peut-être plus subtile de dissuasion réside dans la minimisation des effets qui ne représentent donc plus véritablement d'intérêt pour l'acteur – sans pour autant présenter cependant de véritable danger - de sorte que celui-ci renonce de lui-même à réaliser l'action envisagée.

814. La dissuasion suppose donc une évaluation minutieuse des gains et des pertes, qui peut-être rendue plus difficile dans le cadre numérique en raison des multiples paramètres. En outre, l'une des difficultés supplémentaires peut être la psychologie imprévisible des agents et des mentalités diverses. Ce que risquerait de minimiser une conception trop simplifiée du choix

[475] Lawrence FREEDMAN , *Deterrenc*e, Cambridge, Polity Press, 2004.

rationnel qui négligeait des postures psychologiques irrationnelles mais qui existent bel et bien et des conduites destructrices ou suicidaires.

815. On peut, par exemple, imaginer que, pour des raisons d'orgueil personnel (ou national), un agent persiste dans son action, alors même qu'il n'en a aucunement intérêt voire qu'il y ait pour lui un très grand désavantage à le faire.

Dans le cadre de la guerre froide, tout de même assez particulier, c'est la gravité extrême de la menace qui assure l'efficacité de la dissuasion, à savoir une guerre nucléaire. Nous sommes presque dans une logique du tout rien.

A l'évidence, la dissuasion a également un sens lorsqu'il s'agit de points mineurs ou en tout cas d'importance moins vitale. Or, c'est surtout « au bord du gouffre » si l'on ose dire que la dissuasion marche bien ou du moins le mieux possible. En effet, lorsque le risque est mineur (ou le moindre avantage peu frustrant), l'impact semble plus limité sur le choix fait.

816. Dans le cas des menaces numériques, la dissidence s'avère très complexe[476]. Ceci, pour plusieurs raisons : notamment, les différents dilemmes politiques et stratégiques difficiles à évaluer. Par exemple, parmi des agresseurs potentiels se trouvent des acteurs non étatiques avec des intérêts disymétriques qu'il n'est pas facile de mesurer et de préciser. Hors du cadre étatique, en s'élargissant, la notion même de dissuasion risque de se dissoudre en une série d'éléments algorithmiques assez aléatoires[477].

817. La complexité d'une telle dissuasion tient aussi au fait que, sauf exception – nous l'avons vu - les cyberopérations n'atteignent pas le stade de gravité qui les assimileraient à des agressions armées. Le seuil de représailles n'étant pas facile à mesurer, cela compromet la pratique de la dissuasion. De toute manière, l'absence de tables d'équivalence partagées (en vue de qualifier de façon rigoureuse et la plus objective possible les attaques numériques et informationnelles) ne peut qu'augmenter le risque d'incompréhension et de malentendus. Toutefois, il faut aussi se souvenir que sous l'influence bien inspirée des Etats-Unis, la France et d'autres pays ont adopté un important principe d'équivalence (selon lequel une agression serait jugée en fonction de ses conséquences, afin d'évaluer la pertinence, la possibilité et l'opportunité d'une éventuelle riposte conventionnelle).

---

[476] T.V. PAUL, Patrick MORGAN, James J.WIRTZ*, Complex Deterrence : Strategy in the Global Age*, Chicago, Chicago University Press, 2009.

[477] Alex S. WILNER, « Deterring the Undeterrable : Coercion, Denial and Delegitimization in Counterterrorism » in *Journal of Strategic Studies*, 2011, 34, 1, 3-37.

818. On peut envisager cependant une autre façon de pratiquer la dissuasion que l'on appelle quelquefois la dissuasion ponctuelle[478]. Il s'agirait en l'occurrence non pas tant de dissuader des actes individuels que des séries d'actions dont aucune prise en elle-même n'excède un certain seuil de tolérabilité mais dont l'effet cumulé en revanche finit par former un ensemble que l'on peut juger inacceptable. Ainsi, il ne s'agirait pas tant de fixer des seuils que de jauger des tendances, et surtout de se livrer patiemment à une analyse à long terme intégrant simultanément trois variables : l'intensité, la durée et les conséquences (dommages provoqués). Bien entendu, il ne s'agit de riposter à chaque attaque - ou à chaque opération, mais seulement lorsque leur répétition provoquerait une sorte de saturation et un point de non-retour. À notre sens, cela ne résout cependant pas les problèmes que l'on tente de surmonter. En effet, même s'il ne s'agit plus de fixer un seuil, mais de déterminer une signification globale, il n'en demeure pas moins que des critères doivent aussi être envisagés.

819. Un mot peut encore être dit de la dissuasion par interdiction. Celle qui veut persuader que son opération éventuelle est de toute façon vouée à l'échec[479]. Elle demande une mise en place minutieuse et très soignée. Elle se présente donc comme fort coûteuse impliquant, notamment, le cloisonnement des réseaux, la duplication des systèmes et la diffusion de normes de sécurité opérationnelles. Or, le domaine concerné, celui du numérique paraît soumis à la loi des rendements décroissants ce qui ne favorise pas un tel investissement dans la dissuasion par interdiction.

820. La voie de la coercition semble plus aisée à définir et à réaliser du point de vue technique. Il faut savoir que la théorie de la coercition[480] se développe surtout autour de trois axes. Premièrement, elle consiste à user de menaces et même dans certaines limites de la force pour agir sur la conduite d'un acteur. Dit peut-être plus simplement, il s'agit de persuader la cible de stopper une action négative voire de l'inciter à en choisir, en revanche, une autre favorable. Deuxièmement, la coercition repose bien sur deux facteurs importants qui la conditionnent. D'une part, elle doit être persuasive, autrement dit être crédible en soi. D'autre part, elle doit avoir un impact concret et non seulement théorique. Sa crédibilité ne doit pas seulement être abstraite et dans l'absolu mais elle doit s'appliquer précisément à une situation donnée, en fonction de toutes les variables.

---

[478] Lucas KELLO*, The Virtual Weapon and International Order*, New Haven, Yale University Press, 2017.
[479] Martin LIBICKI*, Cyberdeterrence and Cyberwar*, Santa Monica, RAND Corporation, 2009.
[480] Thomas SCHELLING, *Arms and Influence,* New Haven, Yale University Press, 1996.

821. Enfin, elle doit évaluer les coûts prohibitifs et les dommages collatéraux, auxquels doit se résigner un acteur qui renonce. Ils peuvent être de nature variée, comme l'effritement d'une réputation ou d'une image ou encore le sentiment psychologique d'humiliation. Ainsi, la faisabilité technique n'est pas tout et des paramètres plus relatifs peuvent rendre la coercition moins opérante. Ceci dit, il n'est pas superflu de rappeler que la coercition est devenue un mode d'action souvent utilisé depuis 1945. On observe même une sorte de diplomatie de la coercition qui progresse. On peut songer, par exemple, au développement des régimes de sanctions militaires mais également à des opérations militaires ciblées.

822. La coercition numérique peut emprunter plusieurs chemins à condition de bien connaître et de bien identifier les portes d'entrée et les fragilités. Elles peuvent se réaliser sous formes de menaces ou d'attaques contre l'intégrité des infrastructures ou la conduite des réseaux. Toutefois on peut douter de l'efficacité d'une coercition qui ne causerait pas de dommages suffisamment gênants pour pousser l'acteur à changer de conduite.

    Dans le domaine militaire, il y a des armes en soi très dévastatrices. Il y a aussi des armes cernant précisément leur cible. Lorsque les deux effets sont réunis, cela favorise un effet optimum. Toutefois, dans le cadre numérique, si la cible est cernée avec beaucoup de précision, pour autant les conséquences d'une action menée ne sont en général pas trop effrayantes.

823. Il reste aussi à bien concevoir des signaux convaincants d'une détermination à mener à bien une menace ce qui n'est pas simple. Seul un signal fort est efficace. De fait, les attaques numériques sont en général celles qui n'ont pas été annoncées : comme des actes de sabotage, de subversion ou d'espionnage. Une action est d'autant plus efficace qu'elle est faite par surprise. ce qui ne cadre pas avec la volonté de jouer sur la force d'un signal préalable. Pour autant, l'utilité du recours à la coercition ne saurait pour autant être minimisée.

    En premier lieu, l'efficacité d'un signal ne tient pas seulement ni d'abord à la précision de la formulation de la menace mais peut-être surtout à une réputation d'agresseur déterminé. À la limite, une certaine indécision sur le menu de ce qu'il pourrait faire, risque d'être plus efficace en terme d'impact psychologique.

    En deuxième lieu, l'ambiguïté des tactiques numériques qui ne sont pas toujours faciles à identifier et encore moins à distinguer les unes des autres laisse régner une certaine confusion entre la pénétration des réseaux et l'exploitation de cette pénétration dans des buts négatifs. Cela renforce l'effet coercitif sous forme de chantage flou et d'autant plus déstabilisant. François Mitterrand prêtait au célèbre Cardinal de Retz ces mots qui expriment exactement ce

dont il s'agit : « On ne sort de l'ambiguïté qu'à ses propres dépens ». De fait, une menace globale et vague est d'autant plus redoutable et difficile à conjurer.

824. Enfin, en troisième lieu, l'efficacité des actions numériques dans le cadre de la coercition se trouve renforcée par d'autres moyens plus classiques comme l'éventualité d'opérations militaires conventionnelles. C'est exactement ce qu'on fait les Etats-Unis en Irak[481].

825. On le voit, malgré leurs limites intrinsèques, dissuasion et coercition peuvent contribuer à une stratégie globale ; à condition de bien en user et de les inscrire dans un cadre d'ensemble. Ce cadre est celui de toutes les opérations possibles, défensives et offensives, en réalité complémentaires les unes des autres, plutôt qu'alternatives (qui doivent obéir à une cohérence d'efficacité et de légitimité, pour se protéger, mais aussi anticiper une attaque éventuelle). Le tout dans une zone d'incertitude qui, un peu à l'exemple du fameux théorème d'incertitude Werner Heisenberg en physique, n'a rien d'une limite conjoncturelle (ou simplement transitoire, par exemple) à cause des limites de la portée de notre intelligence. Cependant, il tient au caractère en soi complexe, indécidable, mouvant du domaine concerné. Cela s'accorde mal avec la rigueur et la précision attendues et postulées par le juriste. Toutefois, d'une certaine façon, il est obligé de « faire avec » : d'en tenir compte. Ceci, afin d'avoir une prise réelle - non illusoire - sur les contextes actuel et futur.

[481] Shane HARRIS, *@War. The Rise of the Military-Internet Complex*, Boston, Houghton Mifflin Harcourt, 2014.

Section* II *: Des opérations défensives et offensives

a. *La prévention et la protection.*

826. Depuis que l'humanité existe, il lui est nécessaire et légitime de protéger les artères vitales de son fonctionnement et de ses activités.

En ce sens, la cyberdéfense s'inscrit bien dans une continuité historique[482]. Il suffit donc surtout de protéger ce qui est conçu comme important, on pourrait dire une représentation plutôt qu'une réalité. En France, une ordonnance du 29 décembre 1958, dans le double contexte de la guerre froide et - surtout - d'une guerre d'Algérie en cours (et à un stade critique), explicite la mise en place d'un dispositif moderne des infrastructures critiques. Une activité est vitale. En effet, si elle joue un rôle non négligeable dans la survie du pays à tous égards.

827. L'article L1332-1, du Code de défense précise qu'il s'agit des dispositifs « dont l'indisponibilité risquerait de diminuer de façon importante le potentiel de guerre, la puissance économique, la sécurité ou la capacité de survie de la nation ».

Aujourd'hui plus que jamais, tout ce qui relève de l'information s'inscrit dans une nécessité vitale. A l'Âge de l'Internet, il y a comme une déréalisation de ce qui relève de la nécessité vitale. Elle ne se présente plus tant comme une chose, ou une catégorie, ou un concept clairement circonscrit, mais plutôt comme un élément qui tient son sens même du contexte stratégique et des jeux de communication[483].

828. Il est clair que, depuis quarante ans par exemple, ce qui est vraiment vital et urgent pour une société semble avoir véritablement changé. Certes les ressources ou les infrastructures civiles qui les soutiennent conservent en effet une grande importance (par exemple les usines d'armement), mais ce qui relève de l'information paraît désormais plus primordial encore. L'adjectif qualificatif « critique » (bien entendu au sens de la défense et de la sécurité) prend donc sens, aujourd'hui, en fonction de l'activité de service fournie à la communauté surtout dans un cadre précis, activité hautement numérisée comme chacun sait.

---

[482] Danilo D'ELIA, « Les systèmes d'information d'importance vitale : représentation géopolitique de l'incertitude contemporaine » in collectif, *La cyberdéfense* (op. cit), 167-175.

[483] Olivier PALLUAULT, « La dynamique contemporaine de sécurité et le renouveau de la défense civile américaine sous l'administration Clinton », in *Cultures et Conflits*, 2011, 4, 84, 103-129.

829. Quant à définir les intérêts, en France tout au moins, il n'y a nulle loi qui le fasse. Probablement pour deux raisons. D'une part, ce flou laisse la porte ouverte à des réajustements constants d'une liste qui n'est aucunement close. D'autre part, bien entendu, il faut éviter de donner des points de référence et des repères à l'adversaire, ce qui pourrait lui être utile. Or, l'ensemble des actifs vitaux à protéger est difficile à circonscrire. Il s'inscrit plutôt dans un cadastre évolutif et secret.

830. On peut certainement y inclure données personnelles et professionnelles, sensibles et confidentielles, réseaux industriels et bureautiques et d'autres éléments encore. À une époque où des conflits importants peuvent poindre à l'horizon et où des crispations se multiplient, alors que beaucoup de frontières sont poreuses, l'exigence et l'urgence de la protection de ce qui est vital revêtent un caractère de grand sérieux[484]. Sans doute, la protection, indépendamment même de ce qu'elle exige, au plan technique et financier, ne doit pas paralyser l'activité (pas plus que le confinement, lors de la crise sanitaire du Covid-19). Il est donc impossible de tout protéger comme on le souhaiterait quelquefois. Néanmoins, l'enjeu stratégique de cette protection des éléments est considérable et décisif et au cœur de toute politique défensive[485]. Une politique défensive est évidemment indispensable, par une sécurisation maximale. Elle implique de grandes prouesses techniques et un investissement. Le grand problème de toute stratégie de défense est qu'elle doit chercher à colmater toutes les brèches. Il est impossible de faire face sur tous les fronts. C'est usant et épuisant.

831. Du reste, l'effet de surprise est toujours au cœur d'une attaque et maximalise son succès. C'est pourquoi, toute stratégie de défense doit viser à anticiper les développements postérieurs des moyens de cyberattaque, parfois sous un mode très prospectif. Il s'agit de prévenir ce qui peut surgir sans crier gare et qui placera l'attaque dans une posture d'emblée plus fragile. Ainsi donc, sans relâcher l'effort, il faudra redonner aujourd'hui une nouvelle pertinence au vieux proverbe : « la meilleure défense c'est l'attaque ».

b. L'avantage de l'offensive

832. L'histoire mondiale et surtout l'histoire militaire se présentent bien comme une suite de surprises et d'effets de surprise. Les développements technologiques et numériques peuvent parfois nous donner l'illusion que nous serions à l'abri d'une surprise.

---

[484] Alain COURSAGET, « La sécurité des activités d'importance vitale : premier bilan du SGDSN « , *Sécurité et Stratégie,* 2010, 2, 4, 5-17.
[485] Jean-François DAGUZAN, *La protection des infrastructures critiques. L'enjeu stratégique du XXIe siècle*, AFRI, 2010, XI, 1001-1015.

Toute menace pourrait être identifiée à l'avance par des signaux même ténus. La pandémie du Covid-19 nous rappelle du reste à l'humilité. D'ailleurs, le fait qu'il y ait plus de données et plus d'informations ne signifie évidemment pas qu'il n'y ait plus d'effet de surprise, ni de surprises, surtout mauvaises[486] !

833. Nous ne pouvons ici entrer dans le détail de l'analyse du passé qui nous montre l'importance de la surprise que l'on serait aussi mieux avisé de nommer l'initiative. C'est celui qui a l'initiative qui place d'emblée l'opération sur son propre terrain même s'il s'agit d'un terrain immatériel.

Depuis une dizaine d'années, l'histoire connaît un tournant à ne pas négliger. Depuis les cyberattaques de 2007 en Estonie et le recours au virus Stuxnet en Iran plusieurs fois cités, on assiste à la mise en œuvre bien réelle d'opérations numériques vraiment conséquentes dans des buts tactiques et stratégiques. La cyberguerre a bien lieu contrairement à la guerre de Troie de Jean Giraudoux.

Bien entendu, les cyberattaques doublent souvent d'autres types d'attaques, plus conventionnelles. Ces attaques sont de type offensif et non des répliques. Autrement dit, c'est l'initiative qui paie. Il pourrait être intéressant d'analyser les différents champs d'opération, afin de mieux deviner les attaques réelles ou possibles, car évidemment elles s'inscrivent toujours dans un contexte[487]. Un point est cependant à relever d'emblée.

834. Les cyber offensives participent en général de ce que l'on appelle la manœuvre hybride (qui relève souvent plus de la guérilla imprévisible et polymorphe, que de la guerre bien régulée et davantage prévisible[488]).

Comme l'adjectif qualificatif le suggère finalement de façon assez claire, la manœuvre hybride[489] est fondamentalement une combinaison, une association d'éléments - souvent disparates, dans une perspective opérationnelle (à court terme) et stratégique (à long terme). Qui plus est, les actions régulières et les actions irrégulières s'y côtoient, ce qui semble bien relever d'une sorte de néo-guérilla. Les opérations se placent souvent dans un cadre qui n'est

[486] Philippe SILBERZAHN, « Données, identités et surprise stratégique » in collectif, *La cyberdéfense*, (op. cit) , 189-198.
[487] Anthony NAMOR, « Les opérations numériques dans les conflits contemporains » in collectif, *La cyberdéfense, (op. cit*), 199-208.
[488] Joseph HENROTIN*, Techno-guérilla et guerre hybride*, Paris, Nuvis, 2014.
[489] Elie TENENBAUM, *Partisans et centurions. Histoire de la guerre irrégulière au XXe siècle*, Paris, Perrin, 2018.

pas celui de l'Etat, au travers de structures agiles, souples, liquides pourrait-on dire. Il y a bien entendu une diversité tactique en fonction des contextes.

835. Nous avons parlé précédemment des différentes couches de l'espace géographique du numérique et il est intéressant de noter qu'en général les attaques visent d'une certaine façon toutes les couches mais en privilégiant l'une ou l'autre. Pour donner un exemple, l'attaque contre l'Etat Estonien semblait avoir principalement en vue la couche sémantique, autrement dit la signification, avec un fort impact sur l'opinion.

    En effet, sa force symbolique est énorme. En s'appuyant sur une population russophone sensible aux médias, la Russie entend lancer un message qui fait choc.Celui d'une minorité qui défend son histoire, ses traditions, son existence et sa survie. Une autre initiative vise à brouiller la communication et à isoler un système numérique national du reste du monde. C'est par exemple ce qu'a fait la Libye en 2011, en empêchant les utilisateurs de ses réseaux d'y poster textes ou images.

836. On peut donc parler d'un contrôle drastique de tout le numérique. Plus tard, le gouvernement syrien procède de même grâce à des techniques affinées et plus efficaces. Ainsi, il filtre et il contrôle l'internet de tout son pays, en coupe réglée. Il n'est pas certain que sur le long terme cette stratégie soit vraiment efficace, payante et durable, d'autant plus des contournements sont recherchés et parfois trouvés. Toutefois, un bon exemple nous est donné d'une sorte de prise de contrôle d'un pays. Peut-être plus défensif qu'offensif d'ailleurs, en définitive. Ce qui confirme ses limites.

    Là où la combinaison des attaques numériques et des conventionnelles portent plus de résultat c'est en Géorgie en 2008, et plus encore en Ukraine en 2014. Les attaques ne sont pas forcément très sophistiquées, mais leur combinaison par un effet cumulé déjà évoqué en multiplie les effets et le succès. La Russie parvient à véritablement paralyser un gouvernement et à attaquer des cibles fort judicieusement choisies, comme les sites du gouvernement ou les sites locaux d'information.

    Cette stratégie russe nous semble singulièrement adroite, dans la mesure où elle permet de faire diversion et de faire passer inaperçue l'avancée de ses troupes dans le pays. De plus, il s'agit de présenter l'oléoduc BTC comme moins sûr que l'alternative russe en mettant en valeur les failles du système informatique géorgien. C'est en Ukraine, en 2014, que les Russes se surpassent véritablement. Ils combinent des attaques électroniques classiques (mais

remarquablement menées), avec une sorte de complément numérique de haut niveau, bénéficiant de la compétence des experts. La stratégie russe s'explique en bonne partie parce que l'Ukraine bénéficie alors d'une meilleure connexion que la Géorgie. Il est vrai que six ans ont passé.

837. On peut aussi observer les trois phases du soutien à une phase offensive particulièrement agressive au Libye. Au départ, une tête de pont est établie au travers du rétablissement de réseaux dans l'Est du pays grâce à du matériel acheté par le Qatar. Dans un second temps, un réseau décentralisé est mis en place par l'opposition assurant à la fois la coordination tactique et le lien vers l'extérieur. C'est grâce à ce réseau que se réalise la coordination avec les alliés permettant le choix d'objectifs et la circulation d'informations.

838. On remarque que les nouvelles technologies employées sont plus efficaces qu'une chaîne classique de renseignements, et surtout plus rapides. Bien entendu, les nouveaux atouts numériques s'inscrivent bien dans une démarche offensive. Ce développement de moyens efficaces ne veut toutefois pas dire que tout soit facile et aille sans difficulté, et sans rencontrer de résistance. En effet, des stratégies de contournement et de riposte se mettent rapidement en place. Des moyens utilisés peuvent également être toujours détournés et retournés. Ainsi, le service d'analyse du réseau qui permet de filtrer et de fluidifier le trafic peut servir à le bloquer et à le censurer de l'extérieur. Comme un boomerang, un *malware* envoyé peut être utilisé contre son envoyeur cette fois. Par ailleurs, il faut également souligner qu'une tentative de cybercontrôle d'une zone peut ensuite avoir l'effet pervers d'entraîner aussi une perte de capacité du renseignement.

839. Les armes sont souvent à double tranchant. De plus, les opérations numériques prolongent souvent une guerre électronique déjà commencée. De sorte qu'il ne s'agit peut-être pas véritablement d'une nouvelle guerre, d'un genre inédit, mais de la poursuite en plus sophistiqué : avec de nouveaux moyens de conflits, qui demeurent substantiellement identiques ; avec des questionnements éthiques et juridiques toujours récurrents.

    Si cela est vrai, cela pourrait relativiser la pertinence de penser à nouveau frais, y compris d'un point de vue juridique. La cyberdéfense reviendrait plutôt à prolonger une réflexion plus globale sur les guerres et conflits. Celle-ci éclairerait le cas particulier d'un ajout du numérique qui ne constituerait pas vraiment un nouveau chapitre mais un élément discutable de l'ensemble des chapitres.

840. Le débat peut s'ouvrir. En tous les cas, l'approche doit rester une visée d'ensemble ; être holistique. Ne pas trop segmenter des problèmes. Ce qui ne veut pas dire pour autant que le coefficient « cyber » soit anodin ou insignifiant, bien entendu.

c. Centralité de la question de l'information

841. Dans les conflits, la dimension qui semble devenir aujourd'hui la plus critique, est celle de l'information[490]. Or c'est une dimension – semble-t-il – que les pays occidentaux les plus engagés dans la révolution numérique ont quelquefois négligée, au détriment de questions plus techniques, et finalement peut-être moins angoissantes.

842. La Russie ou la Chine ont d'emblée saisi, quant à elles, l'importance cruciale de cette notion d'information dont le contrôle est essentiel et décisif. C'est l'impact informationnel généré par une attaque qui est souvent le plus important. Il ne s'agit donc plus simplement de protéger un réseau et son fonctionnement mais de veiller à l'intégrité d'un système informationnel en référence bien sûr au contexte, et à l'environnement.

843. L'environnement et la structure sont toujours en interaction. On ne peut contrôler l'un sans contrôler et protéger l'autre. Le plus redoutable est sans doute la combinaison d'attaques informatiques et de diffusions de fausses informations, ou du reste d'informations sensibles vraies dont le dévoilement illégal provoque des effets dévastateurs. À cet égard, nous assistons peut-être à une nouveau type de conflictualité, sinon à une véritable guerre d'un nouveau genre, la guerre de l'information[491], et aussi de l'influence sur l'opinion.

Ce nouveau type de guerre pourrait se rapprocher davantage du *soft power*[492], d'un soft *power* que l'on pourrait aussi qualifier de *smart power*. Il combine adroitement des moyens matériels et des moyens immatériels.

Il s'agit - tout simplement - de mettre sur pied une véritable stratégie d'influence, de différentes façons, mais avec l'appui exceptionnel de la révolution numérique. Si le concept est peut-être assez flou du point de vue purement théorique, la réalité qu'il exprime se révèle facilement dans les cas concrets.

---

[490] Bertrand BOYER, « Les opérations sur l'environnement : la nouvelle guerre de l'information » in collectif, *La cyberdéfense (op.cit),* 209-218.
[491] Martin LIBICKI, *What is Information Warfare ?* Washington DC, National Defense University Press, 1995.
[492] Joseph S. NYE*, Cyberpower*, Cambridge MA, Harvard University, 2010 ; *Soft Power: The Means to Success in World Politics*, New York: Public Affairs, 2004

844. Au fond, d'ailleurs, il s'agit d'un phénomène très ancien, depuis le rusé Ulysse, mais qui n'a eu de cesse de se perfectionner. Il s'illustre par deux orientations principales : d'une part l'acquisition d'informations et d'autre part la destruction, ou la falsification d'informations, évidemment dans un but diffamatoire.

C'est ainsi qu'une certaine supériorité peut être acquise[493]. A partir de la guerre du Golfe, en 1991, cete guerre prend une forme nouvelle. Il s'agit de maîtriser l'information mais aussi de contrôler l'environnement dans lequel se livre une guerre et qui est peut-être décisif pour la suite de cette guerre. Les opérations d'influence agissent bel et bien sur un milieu humain lui-même baignant dans un cyberespace qui le façonne et le conditionne. Cela concerne de plus en plus la planète toute entière. À l'évidence, les opérations numériques ne servent pas simplement à diffuser des messages, comme le font les médias de masse.

Les outils du numérique risquent de contrôler de plus en plus la connaissance des individus, leur compréhension, leurs émotions et leurs décisions, dans un cadre forcément éminemment stratégique, de sorte que l'on approche d'une sorte de « pensée hors limite »[494], mais qui serait un immense champ de forces sinon un champ de bataille.

845. De toute manière, dans le combat numérique de nouvelles méthodologies d'analyse doivent encore se développer pour appréhender un système complexe, mouvant et polymorphe. Foncièrement ambigu aussi. On peut aussi se demander quel visage peut alors avoir un adversaire et quel sens peut avoir l'adversité. Loin de déboucher sur une confiance en un avenir pacifique, cette observation entretient plutôt notre inquiétude sur la possibilité insidieuse d'une sorte de conflit de tous contre tous, mais larvé, feutré, sournois, et en bonne partie insaisissable. C'est au fil parfois inattendu de l'action et de l'évolution parfois déroutante du contexte que la réflexion systématique mais toujours transitoire pourra s'élaborer.

L'ensemble de ces considérations nous incite à mettre tout particulièrement en relief la notion d'information comme telle. Elle est - en définitive - centrale, au-delà des ramifications technologiques. Il ne fait ainsi guère de doute que tel soit l'enjeu de fond de la révolution numérique, et qu'un jour peut-être, c'est par une approche systématique (dont elle serait le pivot) que pourra et devra se constituer une tentative d'unification, même partielle et souple, du droit.

---

[493] François-Bernard HUYGHE, *Histoire des secrets : De la guerre du feu à l'Internet* avec Édith HUYGHE, Paris, Éd. Hazan 2000 ; *L 'Ennemi à l'ère numérique, Chaos, Information, Domination*, Paris, Presses universitaires de France, collection Défense et défis nouveaux, 2001 ; *Gagner les cyberconflits : au-delà du technique*, avec Olivier KEMPF et Nicolas MAZZUCCHI, Paris, Economica, 2015 ; *Désinformation : les armes du faux*, Paris, Armand Colin, 2016 ; *L'art de la guerre idéologique*, Le Cerf, 2019.

[494] Qiao LANG et Wang XIANGSUI*, La guerre hors limites*, Paris, Rivages, 1999.

846. Du reste, les différentes révolutions technologiques déjà survenues et encore à venir laissent deviner une grande accélération des choses avec une dissémination de plus en plus forte malgré le possible contre-feu d'un renforcement de la vigilance des Etats. Il sera certainement indispensable et essentiel d'aborder les questions de manière globale et holistique pour surmonter une balkanisation qui deviendrait vite haineuse et violente.

Cela vaut pour chacun des acteurs et pour chacune des autorités. A toutes les échelles. Donc, bien évidemment aussi pour les Emirats-Arabes-Unis.

CONCLUSION GENERALE

Au terme de ce parcours, au-delà d'une situation déjà existante, et d'un panorama possible des nombreux développements déjà accomplis et en cours, c'est surtout un ensemble de défis à relever qui émergent, d'autant plus complexes et urgents que la situation se présente comme en évolution croissante et accélérée, avec une grande marge d'incertitude et donc des menaces qui se multiplient.

Sans aucun doute, la révolution numérique n'induit pas seulement un certain nombre de changements mais c'est elle crée un nouveau paradigme. Autrement dit, tout semble devoir être pensé autrement dans un monde qui devient autre, bien entendu pour le sociologue ou le philosophe, mais également pour le juriste qui ne saurait se contenter de déduire de principes certes essentiels des règles immuables mais peut-être inadaptées, mal appropriées, voire contre-productives. La tâche est bien entendu vaste et immense et toutes les compétences semblent devoir être sollicitées, les plus différentes. .Le regard de l'historien, celui du géographe, celui du sociologue, celui du philosophe et du moraliste paraissent complémentaires pour aborder les enjeux qui ne sont pas d'abord techniques mais en premier lieu humains et civilisationnels. Ce sont ces enjeux auxquels doit être sensible le juriste qui prend conscience qu'il ne s'agit pas seulement de permettre ou d'interdire dans des proportions variables et discutables en plus, mais de tenter de privilégier et d'encourager un point d'équilibre entre des exigences et des soucis complémentaires et souvent en tension. Il n'est pas superflu de prendre appui sur une histoire à long terme, mais à l'évidence il faut aussi prendre acte de la nouveauté d'une situation que nous qualifierions volontiers de "liquide" autrement dit de mouvante, d'indécise, de contradictoire aussi, et qui ne permet guère l'appréhension rassurante d'une problématique bien définie et d'une réalité consistante et clairement circonscrite. En définitive, nous sommes face non pas au réel compact mais à une circulation d'information avec tout ce que cela implique de fluide, de discutable, d'indécidable mais aussi d'influent, d’explosif parfois, et ô combien. Nous sommes en quelque sorte condamnés à l’incertitude et à une remise en cause constante de ce qui semble acquis.

Notre recherche nous a d'abord permis de mesurer à quel point la révolution numérique encore en cours, qui ne nous a pas encore donné tous ses résultats et n'a pas encore déployé toutes ses conséquences, avance pourtant à pas de géants. Elle reconfigure le monde voire en modifie très profondément le visage, comme si elle nous plongeait dans un nouveau logiciel

qui offre de nouvelles opportunités mais présente également de nouvelles contraintes et de nouvelles menaces, pour chacun individuellement dans le cadre de la cybercriminalité, et pour tous collectivement. Il s'agit presque d'une nouvelle civilisation qui voit le jour même si bien entendu, il y a toujours à la fois continuité et rupture. La révolution numérique est sans doute comparable à l'avènement de l'imprimerie et il s'agit, plus encore que la pandémie du Covid-19 qui vient de frapper le monde, d'un événement mondial. Ce point est du reste très important à souligner. Les frontières classiques sont forcément remises en cause et c'est un nouveau cadastre mental du monde qui se met en forme, avec une remise en cause de fait des frontières traditionnelles, mais peut-être de façon mutante et éphémère. Il semble donc de plus en plus difficile de vouloir répondre aux grands défis posés à un échelon national. Pour deux raisons principales. La première est qu'il s'agit d'un phénomène en soi mondial et qui n'est donc pas propre à un pays, même si bien entendu toute réalité internationale est colorée aussi par le pays dans lequel il prend corps. A cet égard, il faut également tenir compte du fait qu'une situation spécifique, par exemple un retard, est vouée à évoluer et parfois à se transformer en son contraire de même qu'un démarrage lent n'interdit pas forcément par la suite un envol rapide. La seconde, est que freiner ou contrôler internet à l'échelle d'un seul pays risque d'être inefficace, car en lui-même et par lui-même le réseau transcende les frontières de sorte que toute solution à trop petite échelle risque d'être un emplâtre sur une jambe de bois.

Il convient cependant de nuancer peut-être le trait car d'une certaine manière les nouveaux défis posés favorise la nostalgie des Etats souverains et des identités nationales aujourd'hui plus floues. On assiste d'une certaine manière à un relatif retour au rôle de l'Etat national pour mieux contrôler le flux et endiguer la menace. On peut cependant se demander s'il s'agit véritablement d'un nouveau courant de fond où s'il ne s'agit pas plutôt d'un contre-courant, complémentaire, mais qui n'est pas voué à inverser le cours de l'histoire de même que l'exception confirme la règle. Dans l'immédiat cependant, la crise sanitaire du coronavirus risque de renforcer une tendance dirigiste et une société du contrôle et de la surveillance, favorisant un usage pour le moins discutables des nouvelles technologies. D'emblée une première observation semble pouvoir être dégagée de notre recherche. La révolution numérique et ses suites constituent un phénomène global très complexe qui peut donc induire un phénomène mais aussi un autre. Il n'est donc pas simple de résumer la situation et encore moins de prétendre que la révolution numérique conduirait à l'avènement plus ou moins certain d'un monde pire ou d'un monde meilleur, d'un monde plus autoritaire du contrôle ou à l'inverse d'un monde plus libéral favorisant le développement. Du reste des effets paradoxaux peuvent aussi se vérifier à des

échelles de durée différentes. Ainsi l'explosion des *big data* contribue-t-elle autant à favoriser une nouvelle forme de démocratie directe, avec plus de transparence, et une vraie participation de tous, qu'à permettre un contrôle des populations pouvant s'avérer au détriment de leur liberté. Paradoxalement toujours, une grande révolution des moyens peut aussi bien contribuer à telle émergence ou à telle autre. Le prophétisme est de saison mais il n'est pas de bon augure. Et ceci pour la raison qui suit et qui est notre deuxième observation.

Le numérique n'est pas un aérolithe tombé du ciel. Il s'affirme dans un cadre historiquement précis et localement situé, dans un contexte qui agit sur lui autant qu'il ne le transforme. Cela veut dire que le numérique ne produit pas tel ou tel effet par un coup de baguette magique mais selon les volontés politiques et les nombreux facteurs qui participent d'un contexte donné, y compris parfois aléatoires comme un virus. C'est la rencontre entre la nouveauté numérique et un existant lui-même en mouvement qui donne naissance à la société de demain avec ses diverses composantes. Il est parfois tentant de penser que la décision des Etats et des autorités en général s'effacerait en réalité plus ou moins, malgré une présence apparente en surface, au profit d'une sorte de système complexe qui auto-produirait et auto-structurerait le monde de demain. Selon une telle vue des choses, nous serions déterminés par le numérique, devenant ses instruments, sinon des marionnettes. Cela vaudrait en particulier de l'exécutif d'un pays mais aussi du pouvoir judiciaire et des juristes qui sans en prendre conscience seraient instrumentalisés par une sorte d'infrastructure qui commande tout et façonne tout en profondeur. Il y a certainement quelque chose de vrai dans cette vue des choses car sans aucun doute un mode de fonctionnement et un moyen, surtout quand le degré de sophistication est aussi élevé, ne peuvent que façonner les hommes, et donc aussi la société et par là les droirs et règlementations qu'ils finissent par se donner. Néanmoins ce conditionnement ne nous semble pas total mais en interaction constante avec le volontarisme politique, des visions du monde et des valeurs, et aussi les intérêts microcosmiques des individus, si important pour chacun d'entre eux même si c'est parfois de façon inavouée. De cette deuxième observation naît une conviction qui soutient notre réflexion et notre recherche. Loin de nous dispenser de la pensée politique, du discernement éthique et de la codification juridique, l'évolution décisive et profonde induite par cet immense changement de monde sinon de civilisation, les appelle au contraire, non pour donner des recettes toute faîte mais au contraire pour trouver des points d'équilibre qui doivent honorer des soucis essentiels comme l'honnêteté et la transparence, mais aussi le respect de la vie privée et de la confidentialité, ou encore l'idéal démocratique.

De façon presque constante s'affirme alors une double difficulté à affronter. D'une part, nous sommes face à une réalité mouvante ce qui rend singulièrement délicat et aléatoire tout jugement, même en se gardant de l'exaltation comme du catastrophisme. Personne ne peut dire ce que sera demain et d'ailleurs le droit renonce à une telle illusion car son objectif est de dire ce qui doit être (et non ce est ou sera), ou peut-être, plus facilement, ne pas être. Pourtant même cette ambition ne présente rien d'évident en fonction d'un flou qui règne. Que nous cherchons avec d'autres à dissiper il est vrai. D'autre part, même ce flou une fois dissipé – bien partiellement sans doute - concernant la révolution numérique, ses enjeux et ses menaces, il semble très difficile de trancher une question particulière comme par exemple celle du juste équilibre entre la protection de la confidentialité d'un côté, et la liberté d'expression et d'information de l'autre. Il semble que nous soyons déchirés entre deux exigences difficilement conciliables, tiraillés entre deux soucis et des valeurs, en cherchant peut-être un juste milieu, mais qui saura placer le curseur au bon endroit et selon quelles règles ?

La cybercriminalité, déjà très répandue et qui a tout de la marée noire, et la cyberguerre, à l'état plus inchoatif, aux prétentions contestées, mais incluant des risques énormes en regard de ce qui est en jeu, nous obligent à la prévention…difficile, car justement demain n'est pas accessible par une prévision. Il faut tracer de grandes orientations et nous sommes toujours renvoyés à cet héritage du droit écrit et de la jurisprudence qui sans doute ne peuvent pas encore nous éclairer sur de nouvelles questions mais néanmoins sont lourds d'une sagesse séculaire pour aborder de grands enjeux humains et sociaux à certains égards analogues malgré tout, car pour décisif que soit le changement suscité par la révolution numérique, l'homme et ses dimensions restent malgré tous les mêmes. D'anciens dilemmes qui se sont toujours posés, comme entre la sécurité et la liberté par exemple, continuent à se poser même si le contexte est autre et les moyens à la fois plus sophistiqués et complexes. En tout cas, on ne peut approcher la question de la révolution numérique d'un point de vue purement technicien mais au contraire dans une approche juridique prudente, pesée et en même temps pressée par le contexte, et l'ampleur quantitative et qualitative de ce qui est en jeu.

Il nous semble nécessaire, enfin, de formuler trois conclusions, concernant de façon spécifique les EAU en n'oubliant jamais que la révolution numérique est d'abord un phénomène mondial et non pas local ou régional, et qu'il est toujours instructif de considérer les situations des autres pays, dans une visée comparative, afin de mieux dégager des observations concernant notre pays, et surtout des préconisations, car c'est qui semble le plus pressant.

En premier lieu, par son histoire singulière, par sa structure fédérale, par sa jeunesse aussi, puisque son indépendance nationale unifiée comme telle est récente, les EAU se présentent peut-être face à la révolution numérique de façon plus vierge. Ainsi, cette dernière est moins liée à des problèmes récurrents du pays qui la conditionnent, la colorent ou la déforme, comme par exemple, il faut bien le dire, le jacobinisme et le centralisme en France. Il est vrai également que le plein développement d'une culture de la démocratie semblable à celle du monde occidental y est encore à l'état inchoatif. En même temps, le pays a connu un surdéveloppement économique rapide et accéléré à une certaine période qui entre en résonance profonde avec le rythme propre de la révolution numérique. Cette dynamique positive est un grand atout mais donne aussi le vertige de sorte qu'il n'est pas possible d'éluder des questions de fond et des considérations juridiques. Les solutions doivent être trouvées le plus vite possible alors même que c'est plus tard dans l'histoire que les EAU ont pris le train en marche, mais à quelle allure. Cela est vrai aussi concernant un respect toujours meilleur des droits de l'homme, objectif très important pour le pays, qui vise l'exemplarité en la matière. D'une certaine façon, la révolution numérique, si elle fait peser des menaces et des dangers, l'y oblige aussi par sa double culture de la transparence de l'information et d'une participation plus démocratique. Et ces deux axes rejoignent l'orientation politique privilégiée aujourd'hui dans le pays.

En deuxième lieu, en raison du rôle du pétrole, mais aussi de sa localisation, près de zones de conflit et de tension très explosive, les EAU sont d'emblée au cœur d'une internationalisation des choses et moins tentés par un repli de type nationaliste qui peut être caressé par d'anciennes puissances (ou seulement certains de leurs habitants en fait) qui semblent avoir perdu la dimension et le prestige d'un autre temps, comme la France, ce dont le Général de Gaulle déjà faisait le constat désolé. L'importance de l'exportation et des échanges confère à la révolution numérique une prégnance plus grande. L'activisme diplomatique des EAU dans un monde à la fois multipolaire et convulsif, qui pourrait être gagné par la méfiance et par des volontés protectionnistes, surtout après le choc tout récent du Coronavirus, ne pourra que bénéficier des acquis présents et futurs de la révolution technologique et numérique.

En troisième lieu, en partie pour les mêmes raisons, les EAU peuvent être des cibles privilégiées de cyberattaque, La richesse du pays, la présence constante de nombreux étrangers, les potentialités financières, l'apothéose de l'urbanisme font des EAU un espace convoité. La dématérialisation et la déréalisation des échanges et des avancées se prolongent par la

dématérialisation et la déréalisation des attaques et des menaces, ce qui ne signifie nullement qu'elles seraient moins redoutables. Bien au contraire, elles risquent d'être plus nombreuses, plus sournoises, plus inattendues, et surtout difficiles à imputer sans l'ombre d'un doute à un coupable bien précis. Raison de plus sinon d'anticiper - car cela est difficile - mais de prévenir en partie par un ajustement cohérent et précis des ripostes juridiques possibles et des parades techniques et politiques. Le monde est un champ de force, et un pays qui veut y défendre sa place et son rôle doit les identifier et les contrôler le mieux possible.

Aussi, si dans ce monde de plus en plus incertain qui se dessine pour demain, il y a quelque chose de probable c'est bien…son incertitude. Fort justement, Paul Valéry pouvait écrire : « l'imprévu lui-même est en voie de transformation et l'imprévu moderne est presque illimité ». Cette phrase semble sonner le glas de toute prétention des politiques et des juristes de protéger, d'apaiser et d'harmoniser avec efficacement, mesure et pour longtemps, le monde de demain, mais encore ceux qui l'habitent. Du reste, comme semble le laisser augurer l'extension de la cybercriminalité, les parades juridiques risquent bien d'être frappées d'obsolescence et d'inefficacité avant de pouvoir porter leurs fruits, les délinquants voire des terroristes gardant toujours une longueur d'avance. Pourtant notre investigation de cet espace fascinant et inquiétant qui s'ouvre sous nos pas et se modifie sans cesse nous laisse entrevoir de façon moins pessimiste un défi, celui d'une acceptation non résignée de l'incertitude pour tenter sans relâche de la rendre plus humaine, ou moins inhumaine. Et les juristes auront du travail. Aux Emirats comme partout ailleurs dans le monde.

MOTS ET CONCEPTS CLES

- **BIG DATA**

On désigne par ce terme une grande quantité de données qu'un seul outil ou appareil ne peut parvenir à contrôler entièrement. L'explosion quantitative des données numériques a obligé les chercheurs à trouver de nouvelles manières de les gérer et parfois de les traiter. Cela suppose de s'appuyer sur de nouveaux ordres de grandeur concernant la capture, la recherche, le partage, le stockage, l'analyse et la présentation des données. La notion de « Big Data » renvoie ainsi au stockage d'un grand nombre d'informations sur une base numérique. Il faut savoir que nous produisons environ 2,5 trillions d'octets de données tous les jours, aussi bien des messages que nous nous envoyons, des vidéos que nous publions, et même des signaux GPS et des enregistrements transactionnels d'achats en ligne en hausse continue. Ce phénomène d'ensemble qui s'accentue pose des défis technologiques et juridiques évidents.

- **BITCOIN**

Le bitcoin est une monnaie virtuelle créée en 2009 par une personne non identifiée dont le pseudonyme est Satoshi Nakamoto. Contrairement aux monnaies classiques (également appelées *monnaie fiat*), le bitcoin n'est pas émis et administré par une autorité bancaire. Il est émis sur le protocole blockchain du même nom. Cette technologie permet de stocker et de transmettre des informations de manière transparente, sécurisée et surtout sans organe central de contrôle. Il permet d'échapper ainsi au contrôle de l'Etat avec les avantages et aussi les risques. Comme beaucoup d'autres crypto-monnaies, il est mis en circulation via le minage. Les "mineurs" sont des personnes réparties partout dans le monde qui effectuent des calculs mathématiques avec leur matériel informatique pour le réseau bitcoin afin de confirmer les transactions et augmenter leur sécurité. En échange, ils reçoivent des bitcoins, qui peuvent ensuite être convertis en *monnaie fiat* ou être échangés contre d'autres crypto-monnaies sur des plateformes d'échange.L'émission de bitcoins est limitée à 21 millions d'unités, comme il a été prévu dans le code initial. Ce montant devrait être atteint en 2140. Début 2018, le nombre de bitcoin émis a passé la barre des 17 millions, soit 80% du total. Ainsi, le bitcoin se crée à un rythme décroissant même s'il n'est pas encore trop tard pour un acquérir. De plus, comme son émission est finie elle prend sans cesse davantage de valeur. Cependant, avant d'acheter des

bitcoins, il est important de garder à l'esprit que, comme pour tout actif risqué, il ne faut pas investir plus que ce qu'on peut se permettre de perdre. Il n'existe pas de compte bitcoin à proprement parler comme il existe des comptes bancaires. Pour se procurer des bitcoins, il faut ouvrir un compte sur une plateforme d'échange de crypto-monnaies (on en dénombre une centaine aujourd'hui dans le monde). En général, il est possible de les acheter par carte ou par virement bancaire. Les commissions varient également d'une plateforme à l'autre. L'objectif du bitcoin est de faciliter les transactions pair-à-pair. C'est un moyen d'envoyer de l'argent rapidement et avec peu de frais. En effet, puisque les transactions sont effectuées directement entre deux personnes, les intermédiaires qui prélèvent des commissions sont limités. Néanmoins, il est impératif de se souvenir que le bitcoin constitue un investissement risqué car il repose sur un marché non régulé et très fluctuant, dans la mesure om cette monnaie virtuelle n'a pas de cours officiel. Il s'agit d'un environnement informatique qui a ses propres règles, ce qui interpelle le droit.

- **BLOCKCHAIN**

La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Elle est la technologie au cœur du Web Décentralisé et de son corollaire, la finance décentralisée. Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création, qui est ainsi conservée et sécurisée. Du reste, il existe des blockchains publiques, ouvertes à tous, et des blockchains privées, dont l'accès et l'utilisation sont limitées à un certain nombre d'acteurs. Ainsi donc, il est possible de comparer une blockchain publique à un grand livre comptable public, anonyme et surtout infalsifiable, ce qui constitue tout son intérêt spécifique. Elle est apparue en 2008 avec la monnaie numérique bitcoin, développée par un inconnu se présentant sous le pseudonyme Satoshi Nakamoto (voir bitcoin).dont elle constitue l'architecture sous-jacente. Depuis, de nombreux acteurs (entreprises, gouvernements, etc) envisagent l'utilisation de la technologie blockchain pour d'autres cas que la monnaie numérique Toute blockchain publique fonctionne nécessairement avec une monnaie ou un token (jeton) programmable. Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les nœuds du réseau appelés les "mineurs", selon des techniques qui dépendent du type de blockchain. Dans la blockchain du bitcoin cette technique est appelée le "*Proof-of-Work",* preuve de travail, et consiste en la résolution de problèmes algorithmiques. Une fois le bloc validé, il est horodaté

et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau. La blockchain est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier sa validité. Le caractère décentralisé de la blockchain, couplé avec sa sécurité et sa transparence, promet des applications bien plus larges que le domaine monétaire. Les champs d'exploitation sont immenses : banques, assurance, santé et industrie pharmaceutique, *supply chain* de nombreux secteurs (agroalimentaire, luxe, commerce international, distribution, vins, aéronautique, automobile…), industrie musicale, énergie, immobilier, vote. Surtout, la blockchain ouvre la voie d'un nouveau web, le web décentralisé, ce qui inclut des défis redoutables à relever économiques, juridiques, ou même écologiques.

- **CONFIDENTIALITE**

La confidentialité exprime le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé et qu'elle protégée de toute curiosité illégitime. Elle constitue l'une des pierres angulaires de la sécurité de l'information et l'une des raisons d'être des crypto systèmes, rendus possibles dans la pratique par les techniques de la cryptographie moderne, techniques de plus en plus sophistiquées. Elle traduit, en outre, un principe éthique associé à plusieurs professions, notamment dans les domaines de la médecine, du droit, de la vente, de l'informatique, de la religion, du journalisme, etc. En éthique et en droit, certains types de communication entre une personne et un de ces professionnels sont dites « privilégiées », et ne peuvent être discutées avec, ou divulguées à des tierces parties. Dans certaines juridictions où la loi assure une telle confidentialité, des sanctions sont habituellement prévues dans les cas d'infraction. La confidentialité peut être mise en danger par la multiplication et le croisement des données.

- **CONTREFACON**

La contrefaçon consiste en la reproduction, l'imitation ou l'utilisation totale ou partielle d'un droit de propriété intellectuelle sans l'autorisation de son propriétaire. Il peut s'agir d'une marque, d'un modèle, d'un brevet, d'un droit d'auteur, d'un logiciel, d'un circuit intégré ou d'une obtention végétale. Elle punissable mais concrètement favorisée par les développements technologiques.

- **CRYPTOMONNAIES**

Les crypto-monnaies forment un moyen d'échange, créé et stocké de manière électronique sur la Blockchain, reposant sur des techniques de cryptage (procédé de rendre toute information incompréhensible à défaut d'une clé de plus en plus sophistiquée) pour contrôler la création d'unités monétaires et vérifier le transfert de fonds. qui opère indépendamment des banques et des gouvernements. Elle peut être échangée et négociée, comme n'importe quelle devise physique (ou monnaie fiduciaire). Il existe un grand nombre de cryptomonnaies disponibles, chacune ayant ses propres caractéristiques et applications.

- **CYBERCRIMINALITE**

La cybercriminalité est une activité criminelle qui cible ou utilise un ordinateur, un réseau informatique ou un appareil mis en réseau. La plupart des activités cybercriminelles (mais pas toutes) sont commises par des cybercriminels ou des pirates informatiques qui veulent se faire de l'argent, ce qui différencie ces activités du cyberterrorisme, dont le but est autre. Les formes de cybercriminalité sont multiples et la cybercriminalité ne cesse de s'accroître. La lutte notamment préventive contre la cybercriminalité devient une urgence absolue.

- **CYBERSECURITE**

D'une grande importance, croissante, cette exigence recouvre l'ensemble de l'arsenal des moyens de toute nature, y compris législatifs, visant à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. On l'appelle également sécurité informatique ou sécurité des systèmes d'information.

- **DOMOTIQUE**

La domotique se présente comme l'ensemble des techniques de l'électronique, de physique du bâtiment, d'automatisme, de l'informatique et des télécommunications utilisées dans les bâtiments, plus ou moins « interopérables » et permettant de centraliser le contrôle des différents systèmes et sous-systèmes de la maison et de l'entreprise. Elle se présente comme « holiste » à savoir comme un tout qui précède et justifie les parties. Elle est liée à

l'interconnection. Plus simplement, elle illustre combien la révolution numérique est également bénéfique dans le cadre plus intime et à une échelle plus limitée. Le but de la domotique est une simplification de la vie de tous les jours, et de lutter contre les pertes de temps et d'énergie par l'amélioration des fonctions.

- **DONNEES**

Les données semblent constituer aujourd'hui la principale richesse dans notre civilisation numérisée. Une donnée est la représentation d'une information de toute nature et d'importance variable dans un programme : soit dans le texte du programme (code source), soit en mémoire durant l'exécution. Les données peuvent être conservées et classées sous différentes formes : textuelles (chaîne), numériques, images, sons. Du point de vue juridique, eles constituent un élément essentiel à protéger dans la mesure où elles contiennent toujours un contenu informatif, parfois crypté, de nature et d'enjeu diversifiés. La donnée existe indépendamment de sa réception et de son interprétation. Une donnée personnelle est une donnée se rapportant à une personne physique, au moins théoriquement identifiable. Les personnes concernées doivent donc conserver le contrôler des données les concernant. Le droit doit assurer la juste protection de ces données. La grande quantité des données, en développement exponentiel (le « big data ») suppose leur bonne gestion, sans quoi, paradoxalement, le surnombre diminue la quantité d'information accessible. Les données peuvent être traitées, en particulier croisées, pour acquérir ainsi de nouvelles informations surtout par recoupement, ce qui constitue une certaine menace. Le défi de la protection des données invite à s'interroger sur leur nature juridique et en particulier à envisager de les intégrer dans ce qui relève de la propriété.

- **GAFAM**

GAFAM est l'acronyme des géants du Web — Google, Apple, Facebook, Amazon et Microsoft — qui sont les cinq grandes firmes américaines (fondées entre le dernier quart du xxe siècle et le début du xxie siècle) qui dominent le marché du numérique, parfois également nommées les Big Five, ou encore « The Five ». Cet acronyme correspond au sigle GAFA initial, auquel le M signifiant Microsoft a été ajouté. par leur taille. Elles sont particulièrement influentes sur l'Internet américain et européen, tant au niveau économique et politique que social, et sont régulièrement l'objet de critiques ou de poursuites sur le plan fiscal, sur des abus de position dominante et sur le non-respect de la vie privée des internautes. Elles tentent

d’étouffer la concurrence et, en riposte, de nombreuses politiques étatiques, tentent justement de relancer celle-là.

- **INTELLIGENCE ARTIFICIELLE**

On désigne par intelligence artificielle (IA) l'ensemble des théories et des techniques déployées pour acteur des machines capables de simuler l'intelligence humaine. Si la potentialité de l’intelligence artificielle est largement reconnue, beaucoup de questions se posent de savoir par exemple si l’intelligence artificielle pourrait un jour se rebeller contre l’homme. En tout cas, l’intelligence artificielle correspond donc davantage à un ensemble de concepts et de technologies plus qu'à une discipline autonome. Pour contrôler l’intelligence artificielle, mais aussi maximaliser son efficience l’homme a intérêt à cultiver sa propre intelligence humaine et vivante. L’étendue des bienfaits et des menaces liés à l’intelligence artificielle semble encore difficile à évaluer. Mais l’intelligence artificielle constitue déjà un outil extraordinaire qu’il s’agit aussi d’encadrer par le droit.

- **INTERNET DES OBJETS**

Cette extension d’internet forme ou est destinée à former une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables. L’internet des caractérise des objets physiques connectés ayant leur propre identité numérique et capables de communiquer les uns avec les autres. Ce réseau crée en quelque sorte une passerelle entre le monde physique et le monde virtuel. Les objets connectés produisent de grandes quantités de données dont le stockage et le traitement entrent dans le cadre des big data. Par exemple, en logistique, il peut s'agir de capteurs qui servent à la traçabilité des biens pour la gestion des stocks et les acheminements. Ou encore, dans le domaine de l'environnement, il est question de capteurs surveillant la qualité de l'air, la température, le niveau sonore ou l'état d'un bâtiment. L’internet des objets est largement exploité en domotique par exemple pour assurer la sécurité d’une maison ou d’une entreprise. Le recours à l’internet des objets se développe aussi dans le domaine de la santé et du bien-être avec le développement des montres connectées, des bracelets connectés et d'autres capteurs surveillant des constantes vitales. Les objets connectés sont pilotables à distance, le plus souvent à l'aide d'un ordinateur, d'un smartphone ou d'une tablette. Cette connection peut se

faire à l'échelle d'une ville, par exemple pour commander les feux de circulation intelligents qui passent au vert lorsqu'ils détectent le passage d'une voiture. En tout cas, ils permettent de stocker une très grande quantité de données.

- MALWARE

Un malware est un logiciel malveillant ou maliciel, aussi dénommé logiciel nuisible ou programme malveillant ou pourriciel, qui suit un programme sophistiqué et soigneusement développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté/.

- MINAGE

Le minage est une activité stratégique qui consiste, à l'aide de matériel informatique, à enregistrer des transactions sur une blockchain en les rendant immuables.

- NUMERIQUE.

En toute rigueur de terme, on appelle numérique une information qui se présente sous forme de nombres associés à une indication de la grandeur physique à laquelle ils s'appliquent, permettant les calculs, les statistique et la vérification des modèles mathématiques. En ce sens, l'adjectif « numérique » s'oppose en ce sens à « analogique » et « algébrique ». Plus largement, l'adjectif se rapporte à l'ensemble des données, des pratiques et des outils informatiques, traitées par des ordinateurs, et à tout ce qui fait appel à des systèmes électroniques construits sur des fonctions logiques, auxquelles se réduisent les calculs arithmétiques. De façon plus large encore, on parle de révolution numérique ou de culture numérique pour faire référence à l'état actuel d'une civilisation marquée par de très nombreuses mutations induites par le développement des outils et des activités numériques.

- PIRATAGE INFORMATIQUE

Les pirates informatiques tentent de s'approprier des données confidentielles, personnelles, professionnelles ou étatiques, parfois dans un but ludique, mais souvent dans une intention nuisible (comme par exemple dérober de l'argent)..Le piratage informatique ne cesse de se

développer et de trouver de nouveaux procédés. D'ores et déjà, il existe plusieurs méthodes de piratage comme le phishing, le vol de mots de passe, les logiciels malfaisants. Alors que des programmes sont mis en œuvre pour le combattre, le piratage prend souvent d'autres formes. Pour évoquer le piratage informatique on parle souvent de *hacking* même si les deux termes ne sont pas exactement synonymes. Le *hacking* se présente au départ dans une perspective d'expérimentation voire de prouesse. Elle tout cas, le *hacker* cherche à contourner les règles et les protections.

- RESEAU

Un réseau est un ensemble d'éléments informatiques (ordinateur, imprimante, hub, modem.) connectés les uns aux autres. Il a pour rôle et pour effet de permettre la communication rapide et fiable d'informations entre les acteurs du système information. Grâce à la révolution numérique, de nombreux agents – en particulier des personnes physiques – sont reliés entre eux, faisant fi des distances physiques et créant parfois de nouveaux espaces de sociabilité, virtuels. Plus largement, le modèle du « réseau » tend à inspirer un fonctionnement très différent de la vie sociale, de la collaboration économique et de l'échange interpersonnel, à considérer sous de nombreux aspects différents.

- SMART CITY

On peut légitimement penser que les villes de demain seront des villes intelligentes (en anglais *smart cities*) à savoir des villes utilisant les technologies de l'information et de la communication pour améliorer la qualité des services urbains ou réduire leurs coûts .L'objectif de ces villes peut être résumé en 3 points : améliorer le confort des habitants tout en disposant de transports plus efficaces et en respectant l'environnement. Par exemple, une smart city met en place des transports en commun durables et interconnectés afin de diminuer leur empreinte environnementale. Une ville intelligente peut ainsi utiliser nombre d'outils fournissant un incessant flux de données pour réguler le trafic en temps réel et ainsi réussir à le fluidifier. En tout cas, les smart cities s'efforcent de gérer les services publics aussi efficacement que possible et de faciliter la vie dans la ville. L'objectif est d'améliorer la qualité de vie pour tous.

- TRANSHUMANISME

Le transhumanisme se présente comme un mouvement, comme un courant, comme une tendance visant à maximiser l'usage des sciences et des techniques afin d'améliorer la condition humaine par l'augmentation des capacités physiques et mentales des êtres humains, voire la suppression du vieillissement sinon de la mort. Il trace une perspective d'ensemble, très discutée du point de vue philosophique et éthique.

- UBERISATION

Le terme uberisation vient de l'entreprise privée Uber) et désigne ce que l'on appelle aussi la plateformisation. Ce phénomène récent, souvent très controversé, réside en l'utilisation de services permettant aux professionnels et aux clients de se mettre en contact direct, de manière quasi instantanée, grâce à l'utilisation des nouvelles technologies. La mutualisation de la gestion administrative et des infrastructures lourdes permet notamment de réduire le coût de revient de ce type de service ainsi que les poids des formalités pour les usagers, ce qui rend ce système attractif. Les moyens technologiques favorisent l'ubérisation qui s'inscrit de manière plus large dans le cadre de l'économie collaborative et d'une société en réseaux en opposition avec le modèle du salariat classique.

- VIRUS

Un virus informatique se présente comme un automate logiciel autoréplicatif. Certains sont inoffensifs, d'autres contiennent du code malveillant plus ou moins dangereux et dévastateur. Dans tous les cas, un virus informatique est conçu pour se propager sur d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes » à la manière d'un virus biologique. Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Un virus se répand très facilement par tout moyen d'échange de données numériques, comme les réseaux informatiques ou les périphériques de stockage externes (clés USB, disques durs, etc.). Il s'inscrit aussi bien dans de petites entreprises de cybercriminalité que dans le dessein plus vaste du cyberterrorisme

BIBLIOGRAPHIE SELECTIVE

I. BIBLIOGRAPHIE PRINCIPALE

- ABED Ibrahim, « The historical background and constitutional basis to the federation », in Ibrahim ABED et Peter HELLYER (dir.), *United Arab Emirates. A New Perspective*, Londres, Trident Press, 2001, 134 [121-144]);

  AMEGEE Amégée, *La cybersurveillance et le secret professionnel : paradoxes ou contradictions : https://www.droit-technologie.org/wp-content/uploads/2016/11/annexes/dossier/81-1.pdf ;*
- AMMOUS Saifedean, *The Bitcoin Standard. The decentralized alternative to central banking*, Hoboken (New Jersey), 2018 ;
- ANCIAUX Arnaud et FARCHY Joëlle, « Données personnelles et droit de propriété. Quatre chantiers et un enterrement » *in Revue internationale de droit économique*, 2015, 3, 307-331 ;
- ANDERSON Jana et RAINIE Lee, « The future of cloud compujting » : *https://www.pewresearch.org/internet/2010/06/11/the-future-of-cloud-computing/;*
- ARPAGIAN Nicolas, *La cyberguerre : La guerre numérique a commencé*, Paris, Vuibert, 2009 ;
- ARQUILLA John, *Networks and Netwars: The Future of Terror, Crime, and Militancy,* New York, Rand, 2001;
- ARQUILLA John, *Information Strategy and Warfare*, Routledge, Contemporary Security Studies, 2007 ;
- BASDEVANT Adrien et MIGNARD Jean-Pierre, *L'empire des données. Essai sur la société, les algorithmes et la loi,* Paris, Don Quichotte, 2018 ;
- BEAUDE Boris, *Internet. Changer l'espace, changer la société,* Limoges, Editions FYP, 2017 ;
- BECHADE Philippe, *Fake News : Post-vérités et autres écrans de fumée*, Paris, Agora, 2017 ;
- BEIGNIER Bertrand, *Le droit de la personnalité,* Paris, PUF, Que sais-je, 1992 ;
- BENSOUSSAN Alain, « Chacun va devenir le trader de ses données personnelles » in *Archimag*, 274, mai 2014 ;

- BERTHIER Thierry, *Cyberchronique – Décomposition systémique d'une cyberattaque, dissymétries et antifragilité,* Publications de la chaire de cyberstratégie CASTEX, janvier 2014 ;
- BERTRAND André, *Le droit d'auteur et les droits voisins*, Paris, Masson, 1991 ;
- BIGO Didier, « La mondialisation de l'(in)sécurité ?Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation » in *Cultures et Conflits*, 2005, 53-101 ;
- BOMONT Clotilde, « Maîtriser le cloud computing pour assurer sa souveraineté » in *La cyberdéfense (op. cit),* 91-98 ;
- BOULANGER Philippe, *Géographie militaire et géostratégie, enjeux et crises du monde contemporain*, Paris, Armand Colin, collection U., 2011 ;
- BRINT Steven, *In an Age of Experts. The changing Roles of Professionals in Politics and Public Life,* Riverside, UCRiverside, 1996;
- CATTARUZZA Armaël, DANET Didier, LAUDRAIN Arthur et TAILLAT Stéphane, « Sovereignty in Cyberspace. Balkanisation or Democratization », IEE, International Conference on Cyber Conflicts, New York, 2016, 146-154 ;
- CATTARUZZA Armaël, « Quelle souveraineté pour l'espace numérique », in collectif, *La cyberdéfense. Politique de l'espace numérique,* Paris, Armand Colin, 2018, 83, [83-91
- CAZEAUX Guillaume*, Odyssée 2.0. La démocratisation dans la civilisation numérique,* Paris, Armand Collin, 2014 ;
- CHIGNARD Simon, *Open data, comprendre l'ouverture des données publiques,* Limoges, Fyp, 2012 ;
- COLIN Nicolas et VERDIER Henri*, L'âge de la multitude. Entreprendre et gouverner après la révolution numérique,* Paris, Armand Colin, 2015 ; *
- CONTI Grégory et DAVID Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict.* New York, Kopidion Press, 2017 ;
-
- COUDRAY Ludovic, *La protection des données personnelles dans l'Union européenne: Naissance et consécration d'un droit fondamental*, Paris, Éditions Universitaires Européennes, 2010 ;
- DAVIDSON Christopher, « The Emirates of Abu Dhabi and Dubai. Contrasting roles in the international system » in *Aslan Affairs*, 38, 1, mars, 33-48, 2007;
- DECHENAUD David*, Le droit à l'oubli numérique. Données nominatives – approche comparée*, Paris, Larcier, 2015 ;

- DE FILIPPI Primavera et McCARTHY Smari, « Cloud computing : centralization and data sovereignity » in *European Journal of Law and Technology*, 3, 2, 2012 ;
- DENARDIS Laura, *The Global War for Internet Governance*, Yale, Yale University Press, 2014 ;
- DESFORGES Alix, « Les représentations du cyberespace : un outil géopolitique « in *Hérodote*, 2014, 152-153, 67-81 ;
- DESGENS-PASANAU, Guillaume, *La Protection des données à caractère personnel,* Paris, Litec LexisNexis, collection Carré Droit, 2012;
- DOUZET Frédérick, « La géopolitique pour comprendre le cyberespace » , in *Hérodote*, 2014, 152-153, 3-21 ;
- DOUZET Frédérick et TAILLAT Stéphane, « L'affirmation du leadership américain » in collectif, *La cyberdéfense. Politique de l'espace numérique*, Paris, Armand Colin, 2018, 111-122 ;
- EKELAND Ivar, *Le chaos,* Paris, Flammarion, Dominos, 1995 ;
- FAVIER Jacques,TAKKAL BATAILLE Adli, *la monnaie acéphale*, CNRS Éditions, 2017 ;
- FONTANEL Jacques et SUSHCHEVA, Natalia, *La puissance des GAFAM : réalités, apports et dangers*, Paris, La Documentation française, 2019 ;
- GANASCIA Jean-Gabriel*, Intelligence artificielle. Vers une domination programmée*, Paris, Le Cavalier Bleu, 2017 ;
- GARLAND David, « On the concept of moral panic », 2008. *https://journals.sagepub.com/doi/10.1177/1741659007087270*
- GEFFRAY Edouard, « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? » : *https://www.cairn.info/revue-les-nouveaux-cahiers-du-conseil-constitutionnel-2016-3-page-5.htm*
- GILLES William, « Démocratie et données publiques à l'ère des gouvernements ouverts : pour un nouveau contrat de société ? », *in Droit et gouvernance des données publiques ;*
- GOLDSMITH Jack et WU Tim, *Who Controls the Internet ? Illusions of a Bordeless World,* New York, Oxford University Press, 2006 ;
- GREENFIELD Adam*, Everyware: la révolution de l'ubiquité, tr. fr. éd. Fyp, 2007. privées à l'ère du numérique,* les éditions IMODEV, Paris, 2015, 16 [15-32] ;
- HARRIS Shane, *@War. The Rise of Cyber Walfare,* Londres, Headline Publishing, 2014 ;

- HENNION Romain, TOURNIER Hubert, BOURGEOIS Hubert, *Cloud computing : Décider - Concevoir - Piloter - Améliorer,* Paris, Eyrolles, 2012 ;
-
-
- HENROTIN Joseph*, L'art de la guerre à l'âge des réseaux*, Paris, ISTE, 2017 ;
- HVIDT Martin, « Public-private ties and their contribution to development. The case of Dubai » in *Middle Eastern Studies,* 43, 4, juillet 2007, 557-577;
- JEULAND François-Xavier, *La Maison communicante*, Éditions Eyrolles, 2012 ;
- JORION Paul*, La guerre civile numérique*, Paris, Textuel, 2011 ;
- JOURDAIN Patrick et WERY Patrick, *La prescription extinctive - Études de droit comparé,* Louvain, Bruylant, 2010 ;
- KARGER Paul A. et SCHELL Roger A., « Thirty Years Later: Lessons from the Multics Security Evaluation. », in *Annual Computer Security Academical Conferences,* 2002, 119-126 ;
- KAZIM Aqil, *The United Arab Emirates AD 600 to the Present. A socio-discursive Transformation in the Arabian Gulf,* Dubaï, Gulf Book Centre, 2000 ;
- KELLERMAN Aharon, *Geographic Interpretations of the Internet*, Londres, Springer, 2016;
- LE CUN Yann, *Leçon inaugurale au Collège de France :* http://www.college-de-france.fr/site/yann-lecun/inaugural-lecture-2016-02-04-18h00.htm ;
- LEMAN-LANGLOIS Stéphane, *La sociocriminologie,* Montréal, Presses Universitaires de Montréal, 2007 ;
- LIMONIER Kévin, « Des cyberespaces souverains ? Le cas de la Russie », in collectif, *La cyberdéfense, Paris,* Armand Colin, 2018*,* 123-129 ;
- LOCQUENEUX Cédric, *Le Guide de la Maison et des Objets Connectés*, Éditions Eyrolles 2016 ;
- LORENZ Eward N., « Un battement d'aile de papillon au Brésil peut-il déclencher une tornade au Texas ? », in *Alliage,* 22, 1995, 42-45 ;
- LYNN William J., « Defending a New Domain : The Pentagon's Cyberstrategy » in *Foreign Affairs*, 89, 2010, 5, 89-97 ;
- MEAD Walter Russell, « The Return of Geopolitics » in *Foreign Affairs,* 2014, 93, 3 ;
- MISHRA Néha, « Data localization laws in a digital world » in *The Public Sphere Journal*, 2016, 135-158 ;

- MONGIN Dominique, *Les cyberattaques, armes de guerre en temps de paix :* https://www.cairn.info/resume.php?download=1&ID_ARTICLE=ESPRI_1301_0032
- MOREL Camille, « Les câbles sous-marins : un bien commun :mondial ? » in *Etudes,* 2017, 3, 19-28 ;
- MOURON Philippe, « Pour ou contre la patrimonialité des données personnelles » : *https://hal-amu.archives-ouvertes.fr/hal-01823901*
- NOCETTI Julien, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » in collectif, *La cyberdéfense (op. cit),* 130-136 ;
- OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale,* thèse, 2014, Paris 1, disponible en suivant le lien https://tel.archives-ouvertes.fr/tel-01340600 [archive] ;
- PECK Malcolm, "Formation and Evolution of the Federation and its Institutions" in Ibrahim ABED et Peter HELLYER (dir.), *United Arab Emirates. A New Perspective,* Londres, Trident Press, 145-160;
- PLOUIN Guillaume, *Tout sur le Cloud Personnel, Travaillez, stockez, jouez et échangez... dans le nuage*, Paris, Dunod, 2013 ;
- PLOUIN Guillaume, *Cloud Computing, Sécurité, gouvernance du SI hybride et panorama du marché,* 4e éd., Paris, Dunod, 2016 ;
- POZNANSKY Michael et PERKOSKY Evan, « Did the US 'Hack Back' at Russia ? Here is Why it Matters in Cyberwarfare » *in Monkey Cage*, 2018,
- QUOISTIAUX Gilles, *Bitcoin et crypto-monnaies. Le guide pratique de l'investisseur débutant*, Parisj Mardaga, 2019 ;
- RAYMOND Eric S., *Une brève histoire des hackers* : http://www.linux-france.org/article/these/hackers_history/fra_brief_history_of_hackerdom_monoblock.html;
- REY Bénédicte, *La vie privée à l'ère du numérique,* Paris, Sciences Pub, Lavoisier, 2012 ;
- RID Thomas, *Rise of the Machines. A Cybernetic History*, Londres, W.W Norton, 2017 ;
- RID Thomas et HECKER Mark, *War 2.0 : Irregular Warfare in the Information Age,* Santa Barbara, 2009, Praeger ;
- ROCHELANDET Fabrice, E*conomie des données personnelles et de la vie privée,* Paris, Ed. La Découverte, Collection Repères, 2010 ;

- RUTY Erwan, “Le populisme numérique” *https://www.cairn.info/revue-esprit-2018-3-p-14.htm;*

  SCHWARTAU Winn, *Internet and Computer Ethics for Kids*, Paperback, 2001 ;

  STAMBOLIYSKA Rayna, *La face cachée d'internet : hackers, darknet...,* Paris, Larousse ;

  STRUM Philippa, *Beyond Progressivism,* Kansas, University Press of Kansas, 1993, 2017 ;

- SUSLOV Mark et BASIN Mihail, *Eurasia 2.0. Russian Geopolitics in the Age of New Media*, Londres-New York, Lexington Books, 2016 ; .
- TENEZE Nicolas, *Combattre les cyberagrassions*, Paris, Nuvis, 2017 ;
- TILL Nicolas, « La protection des données à caractère personnel » in *Documentaliste-Sciences de l'Information* 2013/3, 62-69 ;
- TRUCHE Pierre,, FAUGERE Jean-Pierre, FLICHY Patrice, « Administration électronique et protection des données personnelles : Livre blanc », *in La Documentation française, février 2002 : https://www.ladocumentationfrancaise.fr/rapports-publics/024000100/index.shtml*
- VALERIANO Brandon et MANESS Ryan, *Cyber War vs Cyber Realities : Cyber Conflict in the International System,* New York, Oxford University Press, 2015 ;
- VENTRE Daniel, « Le cyberespace définitions, représentations » in *Revue de défense nationale*, juin 2012, 33-38 ;
- VERBEEK Peter-Paul, *Moralizing Technology : Understanding and Designing the Morality of Things,* Chicago and London, University of Chicago Press, 2011 ;
- WARF Barney, *Global geographies of the Internet,* Londres, Springer, 2013;
- WATTS Ronald, "Introduction : le fédéralisme à l'ère de la mondialisation" in *Revue internationale des sciences sociales,* 2001/1, 67, 11 [11-55] ;
- WEIMANN Gabriel, *Terror on the Internet : the new arena, the new challenges,* Washington, United States Institute of Peace, 2006 ;
- WILKINSON John C., "Traditional concepts of Territory in South East Arabia", in *Geographical Journal*, 149, 3, 301-315, 1983 ;
- ZETTER Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon,* Londres, Crown Publishing Group, 2014 ;

II. AUTRE BIBLIOGRAPHIE EXPLOITEE

- AL AZRI Sultan, *Unemployed Youth in the UAE. Personal Perceptions*, lnc, Diane Publishing, 2010;
- ALEXANDRE Laurent (avec Jean-Michel BESNIER*), Les robots font-ils l'amour ? Le transhumanisme en 12 questions,* Paris, éd. Dunot, 2016 ;
- ALEXANDRE Laurent, *La guerre des intelligences. Intelligence artificielle versus intelligence humaine,* Paris, Jean-Claude Lattès, 2017 ;
- ATLAS Christian, *Le droit civil*, Paris, PUF, Que sais-je ?, 2004 ;
- ATTALI Jacques, *Vivement après-demain,* Paris, Fayard, 2016 ;
- BABINET Gilles, *L'ère numérique, un nouvel âge de l'humanité,* Paris, Le Passeur, 2016 ;
- BARROCHE Julien, "La subsidiarité. Le principe et l'application", in *Etudes,* Paris, 2008, 6, 408, 777-788 ;
- BARTHALAY Bernard*, Le fédéralisme*, Paris, PUF, 1981 ;
- BARRETT Raymond, *Dubai Dreams. Inside the Kingdom of Bling,* Yarmouth, Nicholas Brealey Publishing, 2010;
- BASTIEN Gilbert, MARAUT Axel et TELLE Benjamin, *Enjeux et perspectives pour les Emirats arabes unis. Et, après le pétrole,* Paris, L'Harmattan, 2005 ;
- BAUMAN, Zygmunt, *La société assiégée*, Paris, Hachette Littératures, 2007 ;
- BERTRAND Louis, « Politiques sociales du handicap et politiques d'insertion : continuités, innovations, convergences « , in *Revue des politiques sociales et familiales*, 2013, 43-53 ;
- BIGOT Laurent, *Fact-checking vs fake news : vérifier pour mieux informer*, Paris, INA Editions, 2019 ;
- BINMORE Ken, *La théorie des jeux : une introduction*, Paris, Arkhè, 2015 ;
- BLOCKCHAIN FRANCE, *La Blockchain décryptée*, Paris, Netexplo, 2016 ;
- BOSTROM Nick, *Superintelligence,* tr.fr., Paris, Dunod, 2015 ;
- BOYER Bertrand, *Cyberstratégie, l'art de la guerre numérique*, Paris, Nuvis, 2012 ;
- BOYER Bertrand, *Cybertactique : conduire la guerre numérique*, Paris, Nuvis, 2014 ;
- CABRILLAC Rémy, *Introduction générale au droit*, Paris, Dalloz, 11e éd., 2011 ;
- CARVALHO PINTO Vania, *Nation-Building State and the Genderframing of Women's Rights in the United Arab Emirates (1971-2009),* Reading, Ithaca Press, 2012;

- CASTELLS Manuel*, L'ère de l'information, I, La société en réseaux*, Paris, Fayard, 1998 ; II*, Le pouvoir de l'identité*, Paris, Fayard, 1999 ; III, *Fin de millénaire*, Paris, Fayard, 1999 ;
- CASTELLS, Manuel *La galaxie internet,* Paris, Fayard, 2001 ;
- CHAOUCHI Hakima, *The Internet of Things.* London, Wiley-ISTE, 2010 ;
- CHOULI, Billal, GOUJON Frédéric, LEPORCHER Yves-Michel*, Les blockchains. De la théorie à la pratique, de l'idée à l'implémentation,* Paris, Ed. Epsilon, 2017 ;
- CLARKE Matthew, « Language policy and language teacher education in the United Arab Emirates » in *Quarterly*, 41, 3, 583-591, 2007;
- CLERGERIE Jean-Louis, *Le principe de subsidiarité*, Paris, Ellipses, col. ' le droit en question', 1997 ;
- COLLOMB Alexis, DE FILIPPI Primavera, SOK Klara, *From IPOs to ICOs : The impact of blockchain technology on financial regulation*, SSRN, 2018 :https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/
- CORM Georges, *Pensée et politique dans le monde arabe. Contextes historiques et problématiques XIXe-XXIe siècles,* Paris, éditions la découverte, 2015 ;
- DAVIDENKOFF Emmanuel*, Le Tsunami numérique. Education : tout va changer, êtes-vous prêts ?,* Paris, Stock, 2014 ;
- DAVIDSON Christopher, *The United Arab Emirates. A Study in Survival,* Boulder, Lynne Renner Press, 2005;
- DESCAMPS Edmond-Antoine, *La Domotique,* Paris Presses universitaires de France, Collection « Que sais-je ? », 1988 ;
- DICK Philip, *Ubik,* tr. fr. Alain Dorémieux, Paris, Robert Laffont, 1970 ;
- DODGE Martin et KITCHIN Rob, *Atlas of Cyberspace*, Londres, Pearson, 2001;
- DOUEIHI Milad, *Qu'est-ce que le numérique?,* Paris, Presses Universitaires de France, 2013;
- EBER Nicolas, *Théorie des jeux,* Paris, Dunod, coll. « Les Topos », 2004 ;
- ELAZAR Daniel Judah, « Fromstatism to federalism : A paradigm shift », in *International Political Science Review,* 1996, 17, 4, 417-429;
- EL HACHANI Mabrouka, "Open data, collectivités et usagers : une dynamique en questions", in *Open data. Accès, territoires, citoyenneté : des problématiques info-communicationnelles*, sous la direction de Françoise PAQUIENSEGUY, Paris, 2016, 1-22 ;
-

- FERRY Luc, *L'innovation destructrice,* Paris, Plon, 2014 ;
- FERRY Luc, *La révolution transhumaniste. Comment la technomédecine et l'ubérisation du monde vont bouleverser nos vies,* Paris, Plon, 2015 ;
- FISHKIN James S., *The Voice of the People: Public Opinion and Democracy*, New Haven and London, Yale University Press, 1995 ;
- FRENAUX Philippe, « Des produits conçus pour ne pas durer », in *Alternatives Economiques,* 305, 1/09/2011, https://www.alternatives-economiques.fr/produits-concus-ne-durer/00043204 ;
-
- FOUCHER Michel, *L'obsession des frontières*, Paris, Librairie Académique Perrin, 2007 ;
- Gaël GIRAUD*, La théorie des jeux*, Paris, Flammarion, coll. « Champs Essai, 2009 ;
- GREENE William, *Econometric Analysis*, Londres, Prentice Hall, 7éd, 2012 ;
- GUERAICHE William, *Géopolitique de Dubai et des Emirats arabes Unis,* Nancy, Arbre bleu éditions, 2014 ;
- GUTTMANN Benjamin (dir.), *The bitcoin Bible. All you need to know about bitcoin,* sd., sl., 2013 ;
- HERARD-BEY Frauke, *From the Trucial States to the United Arab Emirates*, New-York / Londres, Langmann, nouvelle édition 2004;
- HMEHD Choukri, *Les réseaux dormants, contingence et structure* : *https://www.cairn.info/revue-francaise-de-science-politique*-2012-5-page-797.htm
- HUEBNER Jonathan, « A possible declining trend for worldwide innovation », in *Technological forecasting and social change*, 72, 2005, 980-986 ;
- HUYGHE François-Bernard, *Fake news : la grande peur*, Vapress, 2018 ;
- ICHBIAH Daniel et LEFRANC Jean-Michel*, Bitcoin et cryptomonnaies pour les nuls*, Paris, First, 2018 ;
- KANNA Ahmed, *Dubai. The City as Corporation*, Minneapolis, University of Minnesota Press, 2014;
- KHALAF Sulayman, « National dress and the construction of Emirati cultural identity » in *Journal of Human Sciences,* Bahrain University, 11, 230-267, 2005;
- KHAN Salman, *L'éducation réinventée*, Paris, Jean-Claude Lattès, 2013 ;
- KIESOW Rainer Maria*, L'unité du droit*, Paris, EHESS, 2014 ;
- KOENIG Gaspard, *Le révolutionnaire, l'expert et le geek*, Paris, Plon, 2015 ;
- KRIEGEL Blandine, *Droit naturel et droits de l'homme*, Paris, PUF, 1989 ;

- KURZWELL Ray, *La Bible du changement*, tr. Adeline Mesmin, Paris, M21, 2007 ;
- LA CHANCE Michaël, *Matrix. Mythologie de la cyberculture*, Québec, Presses de l'Université Laval, 2006 ;
- LANDEMORE, Helen*, Democratic Reason : Politics, Collective Intelligence and the Rule of the Many*, Yale, 2013 ;
- LEVY Pierre, *Les technologies de l'intelligence,* Paris, La Découverte, 1990 ;
- MALAURIE Philippe, *Droit des personnes : la protection des mineurs et des majeurs, Issy-les-Moulineaux*, LGDJ, 2016 ;
- NASR Vali, *Forces of Fortune: The Rise of the New Muslim Middle Class and What It will Mean for Our World*, New York, Free Press, 2009;
- NORMAND Alexis, *Les Emirats dui Golfe, au défi de l'ouverture*, Paris, L'Harmattan, 2011 ;
- NYE Joseph Samuel, *Soft Power. The Means to Success in Word Politics*, New York, Public Affairs, 2004;
- PENA-VEGA Alfredo, "L'émergence d'un nouveau mode de pensée" in *Hermès / La Revue*, 2011/2, 60, 86-92 ;
- ROBERT Pascal, « Qu'est-ce qu'une technologie intellectuelle », *Communication et langages*, 123, 2000, 97-114 ;
- ROBINSON David, *Town Meeting: Practicing Democracy in Rural New England,* Boston, University of Massachusetts Pressn 2011 ;
- SASSEN Saskia, *La globalisation*, Paris, Gallimard, 2009 ;
- SADIN Eric*, La vie algorythmique : critique de la raison numérique*, Paris, l'Echappée, 2015 ;
- SAPEY Bob, « La politique du handicap : un modèle reposant sur l'autonomie individuelle » in *Informations sociales* 2010/3, 128-137 ;
-
- SERRES Michel, *Petite Poucette*, Paris, Le Pommier, 2012 ;
- SERVET Jean-Michel*, Les monnaies du lien*, Paris, PUL, 2012 ;
- SMYRNAIOS Nikos, *Les GAFAM contre l'internet*, Paris, éditions Ina, 2017 ;
- SOLOVE Daniel, *Nothing to Hide : the false Tradeoff between Privacy and Security*, Yale, Yale Press, 2011;
- STITZIS Stamatios, *Introduction à la philosophie du droit*, Paris, Vuibert, 2011 ; .
-
- TAUBE Michel, *La face cachée des Emirats Arabes Unis*, Paris, Midi, 2019 ;
- TREILLE Jean-Michel, *La Révolution numérique. Réinventons l'avenir,* Paris, Ovadia 2015 ;
- TRUCHET Didier*, Le droit public,* Paris, PUF, 2014 ;

- VERDIER Pierre, « Secret médical et partage des informations » : *https://www.cairn.info/revue-journal-du-droit-des-jeunes*-2007-9-page-8.htm ;
- VERSPIEREN Patrick, « Le secret médical et ses fondements », 2007 : *https://www.cairn.info/revue-laennec-2007-1-page-6.htm#;*
- VU QUANG HIEU Lupu Mihai, *Peer-to-Peer Computing*, New York, Springer Publishing, 2021;
- WALDNER Jean-Baptiste, *Nano-informatique – Inventer l'ordinateur du XXIe siècle,* Paris, Hermès, 2007;
- ZOLLER Elisabeth, *Introduction au droit public*, Paris, Dalloz, 2e éd. 2013.

.

Index alphabétique

Table des matières