Vincent Ubino

L'actualité du droit à la sécurité face aux nouvelles menaces liées au numérique

Mémoire (de fin d'études)

GRIN

Bibliographic information published by the German National Library:

The German National Library lists this publication in the National Bibliography; detailed bibliographic data are available on the Internet at http://dnb.dnb.de .

Imprint:

Copyright © 2015 GRIN Verlag
ISBN: 9783668076327

This book at GRIN:

https://www.grin.com/document/306704

Vincent Ubino

L'actualité du droit à la sécurité face aux nouvelles menaces liées au numérique

GRIN Verlag

Master II - Droits de l'Homme

L'actualité du droit à la sécurité face aux nouvelles menaces liées au numérique

par Vincent UBINO

2014 – 2015

Je tiens à remercier tout particulièrement Madame Geneviève Iacono
pour sa bienveillance, sa disponibilité et ses conseils éclairés.

Je souhaite aussi remercier Monsieur Laurent Bonnelli
pour ses conseils avisés, son temps, et son expertise.

Par ailleurs, je remercie Messieurs Julien Béal-Long et Nicolas Chambardon
pour avoir pris le temps de me conseiller dans ce travail de mémoire.

Enfin, je tiens à remercier ma mère pour m'avoir soutenu tout au long de mes études.

ABREVIATIONS

- **Art./** Article
- **Art. cit/** Article précédemment cité
- **Bibliogr./** Bibliographie
- **CE/** Conseil de l'Europe
- **CEDH/** Cour Européenne des Droits de l'Homme
- **Conv.EDH/** Convention Européenne des Droits de l'Homme
- **C.Pén/** Code Pénal
- **C.Proc.Pén/** Code de Procédure Pénale
- **ONU/** Organisation des Nations Unies
- **OTAN/** Organisation du Traité de l'Atlantique Nord
- **OCDE/** Organisation de Coopération et de Développement Economique
- **CNIL/** Commission Nationale Informatique et Libertés
- **CNCTR/** Commission Nationale de Contrôle des Techniques de Renseignement
- **CNCIS/** Commission Nationale de Contrôles des Interceptions de Sécurité
- ***Ibid*/** *Ibidem* (au même endroit)
- ***Id./*** *Idem* (le même auteur)
- ***Inf./*** *Infra* (ci-dessous)
- ***Loc.Cit*/** *Loco citato* (à l'endroit cité)
- **N°**/Numéro
- **N°s/**Numéros
- ***Op.Cit*/** *Opere citato* (dans l'ouvrage cité)
- **P./** Page
- **S./** Suivant
- **SS./** Suivant(e)s
- **Sup./** *Supra* (ci-dessus)
- **V/** Voir

« *Société et individu : voilà nos deux trésors ;*
et nous devons courir au secours de l'un et de l'autre,
selon le cours des événements. »
Alain.

Introduction

«*(…) La prévention d'atteintes à l'ordre public, notamment d'atteinte à la sécurité des personnes et des biens, [est] nécessaire à la mise en œuvre de principes et droits ayant valeur constitutionnelle* »[1] : le juge constitutionnel, loin d'opposer les deux notions traditionnelles de "*sécurité*" et "*liberté*", rappelait dès 1981 qu'elles entretiennent un rapport complémentaire, sinon nécessaire à la jouissance des droits fondamentaux dans une société démocratique. Cependant, s'il « *(…) n'y a point de mot qui ait reçu plus de différentes significations, et qui ait frappé les esprits de tant de manières, que celui de liberté* [2]», c'est aujourd'hui la sécurité qui par-delà ses implications classiques, suscite des questionnements quant au devenir des droits de l'homme sur le terrain numérique, au regard notamment de ses prolongements contemporains :

Au niveau national, la liberté puise ses origines dans le « *bloc de constitutionnalité*[3] » et résulte directement des textes de la DDHC de 1789, du Préambule de la Constitution de 1946, et de la Constitution de 1958 comme de certains principes dégagés par le juge constitutionnel[4], quand la Conv.EDH[5] et la Charte des droits fondamentaux de l'Union Européenne[6] consacrent principalement son existence juridique au niveau européen et communautaire. Au niveau international, c'est la Déclaration Universelles des Droits de l'Homme de 1948[7] dont les dispositions seront reprises par les deux Pactes Internationaux ayant acquis un force obligatoire, relatifs pour l'un aux Droits Civils et Politiques[8] (PIDCP) et pour l'autre aux Droits Economiques, Sociaux et Culturels[9] (PIDESC) qui en en garantissent l'exercice.

Quand elle est consacrée, la liberté recouvre alors plusieurs réalités : elle renvoie non seulement à un ensemble de droits fondamentaux dont le caractère exigible permet à son titulaire de solliciter l'action des pouvoirs publics, puisque nécessaire à sa réalisation, mais aussi à certaines libertés fondamentales inhérentes à la personne humaine, qui impliqueront cette fois une abstention de toute action des pouvoirs publics

---

[1] Décision du Conseil constitutionnelle de conformité, « *Sécurité et Liberté* », 19 et 20 janvier 1981, n°20-127.
[2] MONTESQUIEU, « *De l'esprit des lois* », Chapitre II du Livre XI, Genève, 1748.
[3] La décision de conformité du Conseil constitutionnel, "Liberté d'association" du 16 juillet 1971 consacre la valeur constitutionnelle du préambule de la Constitution de 1958, lequel renvoie au préambule de la Constitution de 1958 et à la DDHC 1789.
[4] Il s'agit notamment des Principes Fondamentaux Reconnus par les Lois de la République, des principes politiques, économiques et sociaux particulièrement nécessaire à notre temps, ou des principes et objectifs à valeur constitutionnel.
[5] Article 5 *« Toute personne a droit à la liberté à la sûreté. Nul ne peut être privé de sa liberté, sauf dans les cas suivants et selon les voies légales*. »
[6] Chapitre II de la Charte relatif à la liberté.
[7] Article 3 « *Tout individu a droit à la vie, à la liberté et à la sûreté de sa personne* ».
Article 9 « *Nul ne peut être arbitrairement arrêté, détenu ni exilé.* »
[8] Article 9 « *Tout individu a droit à la liberté et à la sécurité de sa personne. Nul ne peut faire l'objet d'une arrestation ou d'une détention arbitraires. Nul ne peut être privé de sa liberté, si ce n'est pour des motifs et conformément à la procédure prévus par la loi.* »
[9] Article I : *« tous les peuples ont le droit de disposer d'eux-mêmes. En vertu de ce droit, ils déterminent librement leur statut politique et assurent librement leur développement économique, social et culturel*. »

susceptibles de s'immiscer dans leur sphère d'exercice pour les citoyens, car relevant par principe de leur intimité. A titre d'exemple, si le droit à l'hébergement d'urgence est une liberté fondamentale au sens du référé-liberté[10], il implique nécessairement que « *(..) Les autorités de l'Etat [mettent…] en œuvre [ce] droit à (..) reconnu par la loi à toute personne sans abri qui se trouve en situation de détresse(…)* [11]*»,* justifiant alors l'exécution d'un acte positif nécessaire à la réalisation du droit. Cependant, la liberté fondamentale d'aller et venir impliquera quant à elle que les autorités de l'Etat ne portent pas atteinte à son étendue[12], prohibant cette fois l'acte positif venant restreindre la plénitude de son exercice, pour autant qu'il soit disproportionné.

Par la suite, ces libertés fondamentales inhérentes à la personne humaine feront progressivement écho à deux conceptions distinctes, selon qu'elles renvoient à la notion de liberté individuelle ou personnelle : la première conception fait l'objet d'une définition stricte au niveau national, et demeure cantonnée au domaine des privations de liberté engendrées par les mesures similaires à la garde à vue depuis la décision du Conseil constitutionnel du 16 juin 1999[13]. Elle nécessite que le juge judiciaire remplisse son « *rôle de gardien de la liberté individuelle* » au sens de l'article 66 de la Constitution, qu'il vérifie ainsi la conformité de ces mesures de contrainte avec le principe de liberté individuelle. La seconde conception fait quant à elle l'objet d'une interprétation plus large : elle ne résulte plus des dispositions de l'article 66 de la Constitution, mais plutôt de celles contenues à l'article 2 de la DDHC de 1789[14]. Elle privilégie le droit à la vie et la liberté de conscience, considérés comme préalables nécessaires à l'exercice de l'ensemble des autres libertés de l'individu, recouvrant notamment la liberté d'aller et venir, le droit à la sûreté, la protection de la vie privée ou la liberté d'expression :

Ainsi entendu, l'ensemble des droits et libertés que recouvre le principe de liberté personnelle s'exerce pleinement, pour autant qu'il ne menace pas l'impératif de sauvegarde de l'ordre public : il s'agit dès lors pour les autorités de police de concilier l'exercice des libertés personnelles avec des considérations de « *sécurité, salubrité, ou tranquillité publique* [15]» dans le cadre des missions de police administrative, ou de tempérer l'exercice de la liberté au regard de l'impératif « *de recherche des auteurs d'infractions, ou de*

[10] L'article l.521-2 du Code de justice administrative : « *Saisi d'une demande en ce sens justifiée par l'urgence, le juge peut ordonner toute les mesures nécessaires à la sauvegarde d'une liberté fondamentale à laquelle une personne de droit public ou un organisme de droit privé chargé de la gestion d'un service public aura porté, dans l'exercice de l'un de ses pouvoirs, une atteinte grave et manifestement illégale (..)* ».

[11] Conseil d'Etat, "*Hébergement d'urgence*", ordonnance du 10 février 2012 AJDI 2012.411

[12] Conseil d'Etat, « *Deperthes* », ordonnance, 9 janvier 2001, n°228928.

[13] Décision de conformité du Conseil constitutionnel, « *Loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs* », n°99-411.

[14] Article 2 : « *Le but de toute association politique est la conservation des droits natures et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression*. »

[15] Article L.2212-2 du Code Général des Collectivités Territoriales : « *Le maire assure le respect de la sécurité, salubrité, tranquillité publique et du bon ordre.* »

sauvegarde de la sécurité des personnes et des biens[16] » dans le cadre des missions de police judiciaire. L'ordre public pose donc les limites de la liberté personnelle, laquelle implique désormais que l'individu n'interfère pas dans les sphères d'exercice des libertés de ses semblables. C'est dire que si l'ordre public vise globalement à prévenir les atteintes aux personnes et aux biens, les libertés personnelles n'auront de limites que celles spécialement impliquées par la sécurité. Or, ce principe de sécurité renvoie aujourd'hui non seulement aux biens propres des individus, recouvrant notamment l'égalité de jouissance des libertés, mais aussi au bien collectif de la société, recouvrant cette fois la normalité de l'exercice des libertés. Dans cette logique, il s'illustre traditionnellement par deux conceptions :

Le principe de sécurité fait classiquement référence au contrat social entre l'individu et l'Etat, pour lequel il s'agira de préserver la liberté, de garantir la propriété, d'instaurer l'égalité fonctionnant sur un système reposant sur le principe de solidarité; mais il renvoie aussi à la police générale dont l'objet est de conserver les biens des personnes cette fois, notamment par l'exercice d'une réglementation et d'une surveillance censée garantir la normalité, fondé sur système reposant plus sur la délation des comportements déviants que sur le principe classique de solidarité. La sécurité, au regard de ses deux implications dans la sphère publique, recouvre donc non seulement une dimension strictement personnelle, mais aussi une réalité collective, quand elle ne renvoie plus seulement au sentiment subjectif, mais revêt aussi une dimension objective : la sécurité, bien que d'origine ancienne, constitue donc surtout un instrument sans cesse réadapté aux évolutions de la société.

L'auteur du "*Contrat social*" est l'un des premiers à définir le concept de "*sécurité*" : tandis que l'étymologie du terme[17] renvoie à l'absence de troubles, elle constitue "(…) *le propre des âmes pures*[18]", et ne pourront alors en bénéficier que "*(...) ceux qui ont la conscience tranquille(...)".* Au sens premier, elle renverrait donc à la nécessaire sagesse de l'homme qui souhaite y prétendre, qui souhaite se mettre à l'abri des menaces. Par la suite, l'Académie française fait évoluer la notion, laquelle renvoie désormais à "(…*) une situation objective, reposant sur des conditions matérielles, économiques, politiques, qui entraîne l'absence de dangers et qui détermine la confiance*"[19] : il s'agit alors moins de caractériser une traditionnelle "*(...) tranquillité intérieure (...), qu'une absence effective de menaces, une situation ou (...) les risques ont été (objectivement) supprimé*s". La notion ne prend plus seulement en compte le comportement de l'individu, mais renvoie désormais aux conditions objectives de vie dans la société : l'absence de sécurité sera alors

[16] Décision de conformité du Conseil constitutionnel, « *Loi d'orientation et de programmation relative à la sécurité* », 18 janvier 1995, n°94-352.
[17] Sécurité provient de *"securus*" : il désigne l'individu qui "*sine*" (sans) "*cura*" (inquiétude).
[18] ROUSSEAU Jean Jacques, "*La nouvelle Héloîse*", Paris, 1817, p.152.
[19] Définition "*sécurité*", dictionnaire de l'Académie française, 1935.

moins la conséquence d'une absence de sagesse personnelle, que le résultat malheureux des lacunes en matière de développement économique et social.

Progressivement, le concept de sécurité va notamment imprégner le droit : elle constitue bientôt "(…) *un élément de l'ordre public matériel, caractérisé par l'absence de périls pour la vie, la liberté ou le droit de propriété des individus*" selon le "*Trésor de la langue française*". La sécurité ne recouvre plus seulement un devoir individuel de sagesse ou une créance exigible de la société, mais bel et bien un droit opposable aux individus ou à l'Etat. La sécurité, au sens juridique, renvoie alors à la "*sécurité publique*" ou à la "*sécurité militaire*", dont l'objet consistera à se prémunir contre la survenance de menaces intérieures ou extérieures. Ainsi, puisque l'autorité publique est désormais garante de la sécurité, ces nouveaux prolongements contemporains vont surtout permettre de lier d'intimité l'individu et l'Etat. Or, dans le souci de préserver le maintien de bonnes relations entre l'autorité publique et sa population, la « *biosécurité*[20] » va spécialement désigner l'"*(...) accompagnement d'une opération de telle sorte qu'elle se déroule sans faille, ni interruption (...) : elle permettra notamment le fonctionnement normal d'une activité, le déroulement normal d'un processus*[21]". La sécurité renvoie alors à un "*droit*"[22] exigible et opposable à l'Etat par les individus, impliquant que l'autorité publique ait tout intérêt pour la sécurité des particuliers, comme pour la sienne, à maintenir un lien suffisamment étroit, voire paternaliste, avec sa population.

Cependant, si ce lien d'intimité a pu être solidement construit au fil des années, le développement de nouvelles activités modifie ces rapports entre l'Etat et la population et nécessite le développement d'un nouveau contrôle, l'exercice d'une nouvelle régulation : l'activité de l'Internet suscite donc mécaniquement l'émergence d'une sécurité « *propre* » à l'activité d'Internet. En effet, les rapports traditionnels entre sécurité et liberté vont être substantiellement affectés par l'émergence de l'Internet qui, s'il constitue le terrain le plus propice à l'exercice des libertés, fait surtout émerger de nouvelles craintes pour la sécurité, tandis qu'il déplace progressivement le curseur de la sphère publique vers la sphère privée, et implique donc de nouveaux compromis dans notre quotidien.

C'est qu'Internet reste avant tout un instrument lié d'intimité avec la sécurité : l'histoire démontre en effet qu'il fût d'abord une innovation censée garantir la sécurité militaire des Alliés dans un contexte conflictuel, par la création de l'ordinateur pendant la Seconde Guerre Mondiale, ou celle d'un réseau de coordination des projets de recherche militaire pendant la guerre froide, avant de constituer un l'instrument contemporain de développement de l'information que nous connaissons :

---

[20] *Op.Cit* "*Le Principe Sécurité*" *Ibidem*....
[21] *Op.Cit* ..."*Le Principe Sécurité*" *Ibidem*.... p.11.
[22] Voir *infra*...Partie I, Titre II, Chapitre I

Durant la Seconde Guerre Mondiale, les armées Allemandes vont développer la machine « *Enigma* », dotée d'un clavier de 26 lettres auxquelles correspondaient 26 ampoules. La logique de cette sorte de machine à écrire consistait à substituer une lettre, reconnaissable grâce à l'une des ampoules allumées, à la lettre effectivement tapée sur le clavier : son objectif était donc de crypter les communications entretenues entre l'Etat-major de l'armée Allemande et les troupes au sol. Les forces alliées vont alors développer la machine « *Colossus* », capable de décrypter ces communications militaires : l'invention constitue notamment le premier embryon d'ordinateur.

Or, cette innovation technologique qui jusqu'alors était de l'apanage exclusif des gouvernements, va être progressivement développée par des entreprises du domaine public : quatre générations d'ordinateurs verront alors le jour, de la création du premier ordinateur électronique par l'entreprise « *IBM* », jusqu'à la dernière génération d'ordinateurs créée en 1981, appelés "*micro-ordinateurs*"[23]. Près de 35ans plus tard, ce sont notamment 64% des ménages Français qui disposent d'un accès Internet, quand 67% de la part de ces ménages utilisent un "*micro-ordinateur*[24]", ou "*Personnal Computer*" (PC). Le développement de ces nouvelles technologies dans le domaine public a en effet conduit l'ordinateur à constituer progressivement le cœur du nouveau système technologique qui s'est mis en place : grâce au développement de l'informatique, les télécommunications sont alors entrées dans l' "*âge d'or des pays industriels*", alors que l'électronique et les satellites permettaient d'acheminer en temps réel des masses d'informations considérables d'un point à un autre de la planète. C'est ce couplage entre informatique et information, ordinateur et téléphonie, qui va notamment donner toute son efficacité au réseau Internet :

A l'origine, celui-ci est mis au point en 1969 par l'Université de Californie à Los Angeles (UCLA) pour coordonner plus efficacement les programmes de recherche américaine en matière spatiale et militaire, avant d'être livré au domaine public quelques années plus tard et d'être officiellement dénommé réseau "Internet" en 1983 : son intérêt est de mettre en contact direct et instantané, un nombre illimité d'intervenants disséminés sur l'ensemble de la planète, en faisant dialoguer des ordinateurs par le biais de l'utilisation des réseaux de téléphonie. Le réseau connaît alors un tel développement, que s'il relie cinq millions d'ordinateurs en 1995, ce sont bientôt dix millions d'ordinateurs qui dialoguent sur la toile d'Internet en 1999[25], tandis qu'aujourd'hui, le nombre d'internautes avoisine les trois milliards d'utilisateurs[26].

---

[23] BERSTEIN Serge et MILZA Pierre, "*Histoire du XXème siècle : la fin du monde bipolaire, Tome 3*", Editions Hatier, 2010.
[24] Enquête de l'Institut National des Statistiques et Etudes Economiques (INSEE), « *Internet de plus en plus prisé, l'internaute de plus en plus mobile* », GOMBAULT Vincent, Division Conditions de vie des ménages.
[25] *Op.Cit*..."*Histoire du XXème siècle : la fin du monde bipolaire*" *Ibidem*...p.35 et ss.
[26] Etude "I*nternational Union of Telecommunications : World Telecommunications/ ITC Indicator Datah*", 12 mai 2014, disponible sur le site : wwww.lemondeinformatique.fr.

A la genèse du réseau Internet, l'objectif consistait donc à développer des machines objets fonctionnant de manière autonome : "*Colossus*" devait déchiffrer de manière autonome les communications cryptées d'"*Enigma*", quand les PC devaient fonctionner de manière autonome pour permettre aux intervenants de communiquer librement entre eux. Dès lors, afin de fluidifier l'utilisation du réseau, il ne s'agissait plus seulement de promouvoir une production quantitative, mais plutôt de mettre l'accent sur une production qualitative : ces progrès ont notamment permis de développer l'intelligence artificielle.

On retrouve actuellement l'intelligence artificielle dans les domaines les plus divers : elle concerne aussi bien les activités de loisir permettant de mesurer la performance réalisée lors d'un exercice physique, que le domaine de la santé avec la mise sur marché de nombreux dispositifs permettant de prévenir les maladies chroniques[27]. Surtout, la livraison du réseau Internet au domaine public, la démocratisation de son usage dans la société, conduit à introduire ces nouvelles technologies intelligentes dans la sphère privée : elles sont aujourd'hui en interaction avec une part toujours plus grande de notre intimité.

Dans le domaine du logement se développent ainsi des *"compteurs intelligent*s" qui visent à réaliser des économies d'énergie, à développer des lieux d'habitation toujours plus adaptés aux besoins des occupants, sinon au confort des résidents : ce nouveau type de "*maison connectée*" permet ainsi de programmer, à partir d'un unique système d'exploitation, l'ensemble des appareils domestiques, la consommation d'électricité et d'énergie ou encore la sécurité du logement. Plus encore dans notre sphère privée, la *"voiture connectée*" permet, grâce ses capteurs détectant l'usure de l'ensemble de ses composantes ou d'objets communiquant directement avec les autres véhicules, de renforcer la sécurité, d'accéder à l'ensemble des contenus aujourd'hui disponibles sur nos tablettes électroniques ou "*téléphones intelligents*"[28] ("*smartphone*").

L'ensemble de ces appareils connectés suscite non seulement un nombre toujours plus important d'utilisateurs d'Internet, mais génère mécaniquement un nombre exorbitant de données : le terme « *Big Data*[29] » ou « *numérique »* fait alors référence à cet ensemble d'informations.

La notion s'entend traditionnellement comme la représentation d'une information par un nombre fini de valeurs représentées le plus souvent de manière binaire, par une suite de 0 à 1. Cette nouvelle logique d'identification permet alors non seulement d'exprimer des réalités différentes dans un langage universel, comme la suite binaire, mais plus encore de traiter ces informations de manière systématique, afin de les mettre en relation. Ainsi, selon les termes du philosophe Bernard Stiegler, le numérique s'entend comme le processus "*grammatisation du réel*" qui conduit à développer une "(…) *description de formalisation et de*

[27] Etude annuelle, Conseil d'Etat, "*Le numérique et les droits fondamentaux*", 2014, p.160 et ss.
Disponible sur le site : www.ladocumentationfrançaise.fr
[28] *Op.cit* ... "*Le numérique et les droits fondamentaux*" *Loc.Cit*...
[29] Voir *infra*... Partie I, Titre I, Chapitre I, Section I.

discrétisation des comportements humains permettant leur reproductibilité"[30]. Surtout, si le développement du numérique engendre des évolutions technologiques considérables, pose de nouvelles questions philosophiques, il conduit plus encore à modifier les conditions de vie économiques et sociales dans nos sociétés en prévenant un nombre considérable de risques contemporains[31] : or, si "*(...)les risques peuvent résulter de catastrophes naturelles ou sanitaires appelant des réponses à l'échelle mondiale(...), la menace peut quant à elle provenir [non seulement] d'Etats et de groupes non étatiques transnationaux (...)*[32]" mais aussi d'individus associés[33], ou isolés[34]. Les technologies du numérique, si elles permettent aujourd'hui de prévenir une palette considérable de risques, selon qu'ils soient collectifs ou individuels, ou interviennent dans notre environnement ou dans notre quotidien[35], doivent alors faire face à ces nouvelles menaces pour un certain nombre de libertés classiques dans un monde "*gouverné par les données*"[36].

C'est que la multiplication des "*objets connectés*" ou *"learning machines*[37]", conduit au développement d'une autoréglementation de notre quotidien dans un souci de confort : il s'agit de privilégier l'accès aux comptes bancaires ou l'achat de produits via un ordinateur ou téléphone, plutôt que d'opter pour le déplacement physique ; de privilégier la communication instantanée par écrans interposés, plutôt que la rencontre spontanée. L'objectif des pouvoirs publics sera alors de sécuriser l'activité, dans le but de disposer de l'ensemble des nouvelles technologies de l'Internet, de permettre au citoyen de jouir de l'ensemble des droits et libertés numériques. Cependant, cette logique conduit à l'immixtion progressive de la sécurité dans notre intimité et si la sécurité constitue aujourd'hui moins un droit personnel, qu'un droit de l'Etat, c'est progressivement l'objectif de régulation d'une activité normale dans notre quotidien qui est recherchée, sinon le déroulement normal du processus de loyauté envers les autorités qui est servi.

Dès lors, si la "*sécurité constitue (bien) la première de nos libertés, une garantie d'égalité*" lorsqu'elle permet de réaliser des progrès en matière de prévention des risques sanitaires, des catastrophes naturelles, ou des atteintes à l'ordre public[38] justifiés par des motifs de poursuite de l'intérêt général, elle représente néanmoins une menace pour l'exercice de certaines libertés traditionnelles quant à elle vise à assurer le fonctionnement *"normal"* des activités liées au numérique. Menace d'autant plus dangereuse, que si l'on suit

[30] STIEGLER Bertrand, "*Social Networking as a Stage of Grammatization and the New Political Question*", 2013, 460 pp.
[31] Voir *infra*...Titre I, Chapitre I, Section I, Sous-section 2.
[32] Livre Blanc de la "*Défense et Sécurité Nationale*", "*La Documentation Française*", juin 2008.
[33] On parle notamment d'"*association de malfaiteurs*" qui vise, selon les dispositions de l'article 450-1 du code pénal "*(..) tout groupement ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits (...)*"
[34] L'article 5 de la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme incrimine désormais l'entreprise terroriste individuelle par exemple.
[35] Voir *infra*...Titre I, Chapitre II, Section II
[36] Voir *infra*...Titre I, Chapitre I, Section I, Sous-section I.
[37] Voir *infra*...Titre I, Chapitre II, Section I, Sous-section 2.
[38] Voir *infra*...Partie I, Titre I, Chapitre I

la logique de Michel Foucault selon laquelle c'est la notion de *"déviance"* qui permettrait finalement de caractériser la normalité[39], d'exclure ou d'inclure l'individu dans l'ordre social, elle implique la mise en place de dispositif censés garantir spécialement cette normalité, sinon l'assurance de la loyauté des citoyens envers les autorités publiques : à ce titre, elle reste un instrument politique.

Le développement du premier de ces dispositifs correspond à la première affirmation d'un « *droit fondamental à la sécurité* » dans le langage juridique. En 1995, la loi relative à la vidéosurveillance dispose que « *la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives*[40] » : tandis que le principe sera transposé dans le code de la sécurité intérieure, il justifiera nécessairement le déploiement de dispositifs propres à assurer cette sécurité dans tous les domaines ou sont susceptibles de siéger nos libertés individuelles et collectives. Or, ces dispositifs s'ils sont toujours plus contraignants, deviennent aussi de plus en plus intrusifs dans notre vie privée grâce aux technologies du numérique qui recueillent, collectent un ensemble toujours plus exorbitant de données personnelles, d'informations sensibles nous concernant : le « *Big Data* » favorise ainsi le développement de ce qu'on appelle bientôt les « *sociétés de contrôle* »[41].

Or, dans un tel espace que celui de l'Internet, l'actualité démontre qu'il est aujourd'hui complexe de concilier plusieurs objectifs dans nos sociétés contemporaines : il est non seulement primordial d'assurer la protection des droits et libertés fondamentaux sur le terrain numérique, ou la sécurité juridique des utilisateurs du réseau Internet d'une part, mais aussi nécessaire d'instaurer un contrôle de l'activité numérique, d'exercer une sécurité policière permettant un usage d'Internet conforme aux droits et libertés d'autrui d'autre part. La sécurité policière doit ainsi permettre de préserver la sécurité juridique. Aussi, tandis que le numérique interfère de plus en plus avec nos sphères intimes, ou qu'il permet de réaliser des progrès considérables en matière de prévention des risques contemporains, la question de l'utilité du stockage de nos données personnelles se heurte au principe de protection de notre vie privée : il s'agit alors de concilier la poursuite d'un intérêt général avec la préservation de notre intérêt personnel, tandis que les deux sphères traditionnelles du public et du privé se confondent aujourd'hui sur le terrain de l'Internet.

Cependant, c'est l'émergence de nouvelles menaces numériques qui semblent paradoxalement poser les premiers jalons d'une régulation au sein des rapports entre nécessité du contrôle, instauration de l'ordre et poursuite de l'intérêt public d'une part et protection des droits fondamentaux, préservation de la liberté et sauvegarde des intérêts privés d'autre part : c'est que les menaces numériques ont de commun leur atteinte à la sécurité juridique et policière, quand elles violent non seulement le droit une sécurité personnelle

[39] FOUCAULT Michel, "*Histoire de la folie à l'âge classique*", Editions Gallimard Essais, 1972.
[40] Voir *infra*…Partie I, Titre II, Chapitre I, Section II
[41] DELEUZE Gilles, « *Post scriptum sur les sociétés de contrôle* », « *L'autre journal* », n°, mai 1990.

invocable par l'individu, mais aussi le droit à une sécurité intérieure, invocable cette fois par l'Etat. Ainsi, tandis que les menaces numériques se distinguaient principalement selon leur objectif, tenant soit à cibler directement les systèmes d'information, soit à utiliser ces systèmes pour cibler les individus, une nouvelle catégorie peut aujourd'hui être employée afin de regrouper l'ensemble de ces menaces dans un contexte de développement des technologies de l'information et de la communication : l' « *atteinte informationnelle* ».

Cette nouvelle catégorie permet notamment d'appréhender l'ensemble des menaces numériques, mais aussi de distinguer en son sein des menaces particulières selon qu'elles visent déjà à propager, diffuser des informations sensibles[42], ou qu'elles visent cette fois à recueillir, récolter des informations sensibles[43] : surtout, elles permettent d'appréhender un type spécifique de menace numérique qui donne toute son actualité à la question de la régulation de l'activité Internet, sinon à celle de la conciliation entre préservation de l'exercice des libertés personnelles (notamment la protection de la vie privée, la liberté d'expression sur le terrain numérique) et la poursuite du maintien de l'ordre intérieur : la menace terroriste.

Quand le numérique a de particulier sa faculté à transcender les frontières, l'expansion de l'Organisation de l'Etat Islamique (« *Daech* » ou « *O.E.I* ») a d'inquiétant sa capacité à toucher le terrain physique, mais aussi virtuel. Dès lors, s'il s'agit moins pour les terroristes de combattre les armes à la main, qu'avec un téléphone dans l'une et l'arme dans l'autre[44], le territoire décentralisé de l'Internet constitue potentiellement une zone de non droit, propice à l'émergence de nouvelles menaces pour la sécurité intérieure du territoire national. Cependant, tandis que le Premier ministre rappelait encore devant l'Assemblée Nationale que « *(...)les djihadistes ont parfaitement intégré la révolution numérique* », les pouvoirs publics ont alors déployé de nouveaux moyens propres à lutter contre l'émergence de ces nouvelles menaces « *cyber-terroristes* »[45], parmi lesquelles figure le projet de loi sur le renseignement.

Bien que le projet de loi sur le renseignement vise à répondre à des besoins de sécurité conjoncturels, son adoption définitive implique des changements structurels non seulement pour l'exercice des libertés personnelles, mais encore pour le choix de l'utilisation de l'outil numérique que la société est prête à privilégier. Ainsi, si elle devra choisir à l'avenir entre le privilège de la sécurité policière, ou le privilège de la sécurité juridique, elle laisse surtout en suspens plusieurs questions fondamentales aujourd'hui :

[42] Voir *infra*… Partie II, Titre I, Chapitre I, Section I
[43] Voir *infra*… Partie II, Titre I, Chapitre I, Section II
[44] LUIZARD Pierre Jean, « *Le piège Daech , l'Etat islamique ou le retour de l'histoire* », La Découverte, 2015
[45] Voir *infra*… Partie II, Titre I, Chapitre II

Quelle dimension de la sécurité doit-être aujourd'hui préservée sur le terrain numérique ? Le « *droit à la sécurité* » renvoie-t-il plus au contrôle de l'activité du numérique, qu'à la protection des droits et libertés fondamentaux numériques ? Son exercice droit doit-il privilégier la souveraineté de l'individu ou la souveraineté de l'Etat ? S'agit-il finalement de préférer la responsabilité de protéger ou l'opportunité de surveiller ?

Le développement des technologies du numérique, si elles constituent un nouveau vecteur de protection des droits et libertés fondamentaux classiques, ou contemporains (**Partie I**), semblent cependant nécessiter un contrôle de l'activité Internet face aux nouvelles menaces émergeante pour nos sociétés (**Partie II**).

PARTIE I

Le développement de l'univers numérique, nouveau vecteur de protection des droits fondamentaux ?

Sécurité : "Etat d'esprit confiant et tranquille."
(Trésor de la langue française, 1971-1994)

L'émergence du phénomène "*Big Data*" a considérablement modifié les conditions de vie économiques et sociales dans nos sociétés : c'est aujourd'hui l'ensemble des outils traditionnels, mais essentiels au bon fonctionnement de la vie de la Nation, qui doivent s'adapter à ces nouvelles technologies (**Titre I**). Plus encore, la démocratisation de ces technologies du numérique appelle nécessairement à repenser le concept classique de sécurité dans les nouvelles sphères d'interactions sociales (**Titre II**), comme elle conduit inexorablement à remodeler les habitudes, sinon l'"*essence*" même de l'individu moderne (**Titre III**).

TITRE I/ Antinomie du droit, dualité de la société

Le développement des technologies liées au numérique, aussi appelé "*Big Data*", engrange une vague d'innovations sans précédent, dans les domaines les plus divers (**Chapitre I**) : à ce titre, on parle "*quatrième paradigme*" de la science (**Chapitre II**).

Chapitre I/ Emergence du numérique, le phénomène "*Big Data*" :

Le numérique peut être qualifié d'innovation majeure en ce qu'il affecte non seulement la société (***Section I***), mais aussi l'individu : à cet égard, ce sont non seulement les habitudes personnelles qui sont bouleversées, mais plus encore la notion même d'identité traditionnellement entendue qui est remodelée, c'est la sécurité juridique qui est assurée, quand celle collective est développée (***Section II***).

Section 1/ Numérique et société

Nos sociétés contemporaines sont marquées par un stockage exponentiel de données, à tel point que l'on peut parler de "*gouvernance des données*" (*Sous-section 1*), quand leur analyse conduit à identifier, sinon appréhender un nombre toujours plus important de risques, ce qui rend leur survenance "*intolérable*" dans les sociétés modernes (*Sous-section 2*).

§.1/ La « gouvernance des données » :

La croissance combinée du nombre d'utilisateurs d'Internet et des débits de connexion a conduit à une explosion du volume des données transitant sur les réseaux : à cet égard, si le trafic mensuel en 2012 représentait 20 000 fois ce qu'il était en 1996, son taux de croissance augmente de 40% chaque année, ce qui représente un quasi doublement tous les deux ans[46]. Par ailleurs, la capacité à exploiter cette masse exorbitante de données s'est considérablement développée ces dernières années, et a donné naissance à une nouvelle expression : le « *Big Data* ».

L'expression correspond au phénomène d'expansion non seulement du volume de données, mais encore du développement de la capacité à les utiliser. L'analyse de l'ensemble de l'activité sur Internet pourrait alors fournir des indicateurs avancés et fiables pour de nombreuses tendances : à ce titre, l'entreprise « *Google* » utilise depuis 2008 l'ensemble des requêtes formulées sur son moteur de recherche pour détecter les épidémies de grippe avec dix ou quinze jours d'avance sur le réseaux classiques de veille sanitaire, avec des résultats probants jusqu'en 2012[47], quand « le *Billion Price Project* »[48] prévoyait la chute des prix entrainée par la faillite de « *Lehman Brothers »* deux mois avant l'indice officiel.

En France, c'est la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) qui, sur la base du répertoire des actes de soins prodigués à chaque assuré social, a pu confirmer les troubles cardiaques causés par la consommation du Médiator, tandis qu'une étude de l'Union régionale des Caisses d'assurance maladie de Bourgogne évoquait déjà en 1998 les dérives de prescription du médicament[49].

On retrouve encore ce schéma de prévention des risques permis par cette "*gouvernance des données*" dans le film « *Minority Report »*[50], ou une société du futur réussit à éradiquer le meurtre en se dotant d'un système de prévention, détection, et répression appelé « *Précrime* » reposant sur trois « *extras-lucides* » : les prévisions de ces derniers permettent alors aux enquêteurs d'arrêter le « *coupable* » avant tout commencement d'exécution de l'infraction, d'éradiquer bientôt le taux de criminalité et les risques pesant sur cette société.

§.2/ Une société moderne intolérante aux risques

La capacité de prévoir la survenance de l'ensemble des risques conduit d'ailleurs à repenser la notion de société moderne :

---

[46] Etude annuelle du Conseil d'Etat, "*Numérique et droits fondamentaux*", 2014, p.48

[47] GINSBERG. J "*Detecting influenza epidemics using search engine query data* ", Revue Nature, Volume 457, 19 février 2009.

[48] Initiative du « *Massachussets Institue of Technology* » (MIT) permettant d'analyser quotidiennement les prix des biens et services proposés sur internet pour produire un indice d'inflation plus précoce que l'indice officiel.

[49] BABINET Gilles, "*Big Data : penser l'homme et le monde autrement* », Editions « *Le passeur »*, 2015, p.74 et ss.

[50] "*Minority Report*", Steven Spielberg, science -fiction, 2002.

Si le sociologue allemand Ulrich Beck considère qu'il faut penser la société selon les catégories de risques auxquels elle est exposée[51], l'utilisation scientifique des données bouleverse substantiellement les habitudes sociétales. Les sociétés contemporaines sont en effet de plus en plus intolérantes aux risques, alors que le panel de prévisions des catastrophes naturelles ou risques écologiques est de plus en plus développé grâce aux technologies du numérique, ce qui rend la survenance de ces phénomènes de plus en plus incompréhensible. C'est dire qu'il y a progressivement un abandon de la doctrine de l'"*imprévisibilité*" avec encore le principe contemporain de précaution[52], qui exclue la perspective de vivre dans un monde incertain en incitant la société moderne à "*s'interroger sur le niveau de risques qu'elle est prête à accepter, tout en laissant la recherche libre d'avancer*"[53].

Cependant, comme le soulève le sociologue allemand, si "da*ns la modernité avancée, la production sociale de richesses est systématiquement corrélée à la production sociale de risques*", et tandis que le choix de développer les technologies innovantes issues du "*Big Data*" reste de l'apanage des pays les plus industrialisés, le risque apparaît aujourd'hui comme un facteur discriminant entre les sociétés selon qu'elles siègent dans les pays développés, dans les pays en voie de développement (PED) ou dans les pays les moins avancés (PMA).

S'il constitue avant tout un instrument au service de l'intérêt général, le « *Big Data* » permet donc de sauvegarder la sécurité juridique personnelle, comme il conduit à développer la sécurité collective. Cependant, il reste un facteur d'inégalité entre pays plus ou moins développés.

Chapitre II:

Avenir du numérique, le "*quatrième paradigme*"

Le "*Big Data*" s'inscrit avant tout dans le progrès (***Section I***) : en permettant la récolte, le stockage, l'analyse d'un nombre considérable de données, il incite à privilégier une nouvelle approche de la sécurité (***Section II***)

Section I/ Numérique et progrès

Le numérique, s'il inscrit la société dans le progrès par le développement notamment de la science (*Sous-section 1*), suscite néanmoins des questions quant à l'exercice de certaines de nos libertés : à ce titre, il nécessite parallèlement le développement d'une sécurité du progrès (*Sous-section 2*)

[51] BECK Ulrich, "*La société du risque : sur la voie d'une autre modernité*", Editions Champ Essais, 2008.
[52] Appelé "*vorsorgeprinzip*", le principe de précaution est formulé dans les années 1970 par l'Allemand KARL VON MOLTKE dans le cadre de l'étude commandée en 1976 par l'Institut de politique européenne de l'environnement.
[53] CHIRAC Jacques, Déclaration, Salon international de l'alimentation, octobre 2000.

§.1/ Le numérique, vecteur de progrès pour la science :

Le « *Big Data* » a fait entrer la science dans une nouvelle ère[54] : il s'agit dorénavant de mobiliser les ordinateurs, seuls objets capables de traiter les découvertes de façon autonome en cherchant des liens statistiques au sein des milliards de données afin d'en tirer des corrélations[55].

La révolution amorcée par le développement des technologies du numérique va entraîner de profondes mutations de la société : le « *Big Data* » va ainsi permettre non seulement des avancées significatives dans la science descriptive, concernant la documentation et la mise en évidence de ce qui produit dans le présent[56], mais permet encore de diagnostiquer les causes probables de ce qui pourrait arriver dans l'avenir, sur les raisons et la nature d'un événement[57]. Le phénomène permet donc d'inscrire les recherches dans une logique prédictive, entraînant des conséquences majeures dans les domaines sécuritaires et, ou assurantiels[58].

Ces progrès vont notamment permettre de prévenir toujours plus de menaces, sinon d'éradiquer un nombre considérable de risques contemporains : à ce titre, le numérique érige la sécurité juridique et collective, en première garantes de l'exercice des libertés dans le présent, comme dans le futur.

§.2/ Le numérique, outil de confort au quotidien ou menace pour nos libertés ?

Outre ces logiques de révélation et, ou de prédiction, le « *Big Data* » permet aux machines de réagir de façon autonome et décuple le potentiel d'intelligence artificielle :

Le développement du numérique a conduit à élaborer des systèmes pratiquant l'analyse de situations concrètes, capables de commencer une action en fonction de la typologie de données. L'analyse s'apparente à la réflexion, quand l'action se traduit par la réaction, sinon la pro-action des machines, conduisant par exemple l'ordinateur à prévenir l'usager d'un dysfonctionnement lorsque l'infrastructure de son opérateur est tombée en panne. L'enchaînement d'actions ("*révélation-prédiction-pro-action-réaction*") permet aux machines d'être ainsi de plus en plus autonomes, à tel point que l'on parle de « *learning machines*[59] ».

---

[54] HEY Tony, TANSLEU Stewart, TOLLE Kristin, « *The Fouth Paradgim : Data scientific intensive discovery* », Microsoft Research, 2009, 284 p.

[55] Voir Sciences et technologies de l'information et de la communication, « *Big Data – Partie 2 : le 4eme paradigme de la science*. », www.bulletins-électroniques.com.

[56] Par exemple, la « *Nation Security Agency* » (NASA) a publié le 20 janvier 2014 un planisphère animé mettant en évidence le réchauffement climatique, mois après mois depuis 1880 grâce à l'équivalent de 133années de données.

[57] Par exemple, les chercheurs de l'Université du Massachussetts comparent les enregistrements des boîtes noires d'avions ayant eu un accident avec celles de vols n'ayant pas rencontré de problèmes afin de déceler quelles informations diffèrent entre les deux vols, ceci dans le but d'identifier et de comprendre les pannes et incidents susceptibles de produire un crashe d'avions.

[58] Voir à cet égard les travaux réalisés par l'Institut Montparnasse, « *Assurance, prévention, prédiction….Dans l'univers du Big Data* », collection Recherches, www.institut-montparnasse/wp-content/files/Collection_recherches_n_4.pdf.

[59] « *Learning Machine* » : système qui pratique l'analyse de situations à partir de données et qui est capable de commencer une action en fonction des typologies de données.

D'ailleurs, les laboratoires du "*Massachussets Institute of Technology*" (MIT), de « *Google* » et « *Apple* » s'intéressent de plus en plus au potentiel de ces machines, et les innovations prises dans ce domaine telles que le logiciel « *Siri*[60] » pourraient conduire à envisager des machines capables de prédire les actions de l'utilisateur, et de commencer un panel d'actions en parallèle. On peut raisonnablement imaginer aujourd'hui qu'une « *learning machine* » puisse prendre un certain nombre d'actions dans la vie quotidienne de l'utilisateur, allant de la préparation de la playlist que l'utilisateur écoute généralement quand il court, à l'ajout de titres susceptibles d'être appréciés, ou à l'envoi d'un message au colocataire de l'intéressé pour l'avertir que l'utilisateur arrivera à une heure déterminée par le calcul prévisionnel de l'activité physique par exemple[61].

Cependant, le progrès engendré par l'utilisation de telles machines peut poser certaines questions éthiques et s'inscrit aujourd'hui déjà dans la réalité. Dans le cadre d'un procès pour homicide volontaire, un enquêteur avait apporté la preuve que l'accusé avait posé une question au logiciel « *Siri* », ou il précisait avoir besoin de « *(...) cacher le corps de son colocataire* » : la question posée était suffisamment explicite pour illustrer la volonté de l'utilisateur de commettre un homicide avec préméditation sur la personne de son colocataire. Le logiciel sollicité proposait alors tout un panel de solutions à l'intéressé, proposant notamment de cacher le corps dans un marais, réservoir, une fonderie de métaux ou une décharge[62].

En définitive, ce n'est pas l'évolution des technologies du numérique qui façonne la société, mais bien plutôt l'usage que la société choisit d'en faire : la notion fait alors de nouveau écho à la "*sagesse*" de la communauté qui détermine en premier lieu le degré d'exposition qu'elle est prête à accepter devant le risque de survenance des menaces, nécessitant le développement d'une sécurité du progrès.

Section II/ Progrès et sécurité

Les avancées technologiques dans le domaine numérique ont donc permis de créer le nouveau type de logiciel intelligent ("*learning machine*") : cette nouvelle machine intervient notamment en matière de sécurité en permettant l'interpellation prédictive des infracteurs (*Sous-section 1*), comme en matière de sûreté des populations, en prévenant la survenance de catastrophes naturelles. Elle emprunte alors certains caractères propres à la sécurité collective, comme à la sécurité policière (*Sous-section 2*).

(BABINET Gilles, « *Big Data, penser l'homme et le monde autrement* », Editions « *le Passeur* », 2015, p.247.)

[60] « *Siri* » : système vocal d'exploitation des « *Iphones* »et « *Ipads* ».

[61] *Op.Cit*… p.240 et ss.

[62] « *Siri peut peser lourd dans un procès pour meurtre* », Article de presse, section Actualité, thématique Société, rubrique Faits divers, l'express.fr, août 2014.

§.1/ Le logiciel intelligent : nouvel acteur de la sécurité ?

L'ancien premier président du Conseil national du numérique illustre dans son ouvrage les avancées permises par le « *Big Data* » dans le domaine de la sécurité[63] : c'est que l'utilisation du numérique peut permettre de faciliter la gestion locale de la sécurité, notamment par des stratégies de déploiement des forces de l'ordre, ou de mettre en place des dispositifs de sûreté globaux.

En matière de sécurité routière, le modèle classique nécessite de munir chaque feu rouge d'une caméra pour individualiser le comportement des feux, et représente un système coûteux nécessitant probablement plusieurs années de planification et de tests avant de pouvoir être réellement opérationnel. Le modèle de « *Big Data* » présente plusieurs avantages quant à lui : il permettrait notamment de "*...récupérer la trace de nos mobiles individuels que commercialisent les opérateurs télécoms pour prédire et révéler avec précision l'évolution du trafic en temps réel"*»[64]. Ces perspectives ne relèvent pas de l'hypothétique, tandis que des initiatives semblables ont déjà pu être prises dans certaines villes[65].

En matière de sécurité publique, on retrouve des logiques semblables avec des logiciels[66] venant positionner les forces de l'ordre de manière prédictive aux endroits où les crimes sont les plus susceptibles de se produire, par le biais de l'utilisation des données de masse : ils ont notamment permis d'enregistrer des baisses de la criminalité de l'ordre de 13% dans certains districts de Los Angeles.

A cheval entre sécurité publique et routière, les robots peuvent aussi être chargés de suivre tous les véhicules, tandis que leur base de données est régulièrement alimentée d'informations sur les arrestations effectives de délinquants, ce qui leur permet élaborer un dispositif permettant d'observer les modèles de données caractéristiques de comportements suspects. Le logiciel, disposant alors de signatures très fortes de tout ce qui peut prédire l'imminence d'un délit ou d'un crime, peut ainsi révéler l'existence de comportements à forte potentialité criminelle. Cette révélation et, ou prédiction permet ensuite aux autorités de disposer leurs forces disponibles sur le terrain à des endroits stratégiques, afin d'identifier et d'interpeller des modèles caractéristiques de comportements délictueux[67].

Le numérique constitue donc un instrument efficace et nécessaire à l'Etat pour assurer le maintien de l'ordre selon les circonstances locales, l'exercice de la sécurité publique de proximité : à ce titre, il constitue un instrument de la sécurité policière dans nos sociétés contemporaines.

---

[63] *Op.Cit…*, «*Big Data, comprendre l'homme et le monde autrement* » *Ibidem*… p.102 et ss.
[64] *Ibidem*...p.104
[65] La ville de Sao Paulo teste des stratégies de réorganisation du trafic en fonction de ce qui est mesuré, ou de ce qui peut être prévu au regard de la connaissance historique de l'évolution du trafic pour des jours déterminées, à des heures précises.
[66] Comme le logiciel commercialisé par la société « *Prépol* »
Voir à cet égard le documentaire « *Citoyen sous surveillance, un œil sur vous* », Arte +7.
[67] *Ibidem*... p.105 et ss.

§.2/ Le logiciel intelligent : nouvel outil de sûreté pour les populations ?

Ces logiques sécuritaires ne s'inscrivent pas exclusivement dans le cadre répressif mais permettent aussi de prévenir, de protéger la sûreté des populations. Ainsi, l'Etat du Texas et l'Université de Californie et de Los Angeles utilisent ce genre de système de sécurité reposant sur des « *learning machines* », en liaison avec le numéro d'urgence "*911*" : la finalité de l'utilisation des systèmes est de parvenir à définir quelles sont les signatures les plus caractéristiques des appels téléphoniques reçus, et permet de déterminer qu'un homme ayant du mal à s'exprimer signifie qu'il faudrait impérativement prévoir que l'équipe d'intervention emporte un dispositif d'oxygénation par exemple. Aussi, les services d'urgence de la « *situation room* » de la ville de Rio de Janeiro, en superposant des données de pluviométrie peuvent prendre des décisions allant du déclenchement de sirènes d'alerte en cas de glissement de terrain dans les favelas situées dans des zones de relief particulièrement accidenté, à l'envoi d'une patrouille de pompiers à une position stratégique ou prioritaire d'intervention[68]. Les technologies du numérique permettent alors non seulement d'assurer la sécurité dans notre quotidien, mais encore de l'assurer dans notre environnement.

Finalement, le « *Big Data* » constitue bien un outil permettant d'assurer non seulement le progrès dans nos sociétés, mais encore d'asseoir le principe de sécurité : il permet alors de protéger les libertés personnelles des individus, comme d'épauler les pouvoirs publics dans leurs missions de police administrative et judiciaire. Il emprunte autant à la sécurité collective, en assurant la sauvegarde de l'intégrité territoriale, qu'à la sécurité policière, en privilégiant la surveillance locale.

TITRE II/ Intervention de la sécurité classique au sein d'interactions numériques

La question de la sécurité constitue un enjeu majeur dans nos sociétés contemporaines (**Chapitre I**), et fait l'objet de débats dans des domaines de plus en plus nombreux, ce qui suscite de nouvelles problématiques : la plus contemporaine de ces problématiques est aujourd'hui la question de la sécurité sur le terrain numérique (**Chapitre II**).

[68] *Ibidem*....pp.106 et ss.

Chapitre I :

Contemporanéité du droit à la sécurité

La sécurité constitue avant tout un principe classique (***Section I***), avant de constituer un droit au niveau national depuis le milieu des années 1990 (***Section II***) : cependant, son actualité conduit progressivement à parler d'un "*droit fondamental*", réaffirmé plusieurs fois en l'espace d'une dizaine d'années (***Section III***)

Section I/ Les racines contemporaines du « *principe sécurité* »

La sécurité constitue tout autant un bien aux mains de la population, qu'il soit individuel ou collectif (*Sous-section 1*), qu'un devoir à la charge des autorités policières et, ou militaires (*Sous-section 2*)

§.1/ La sécurité en tant que bien : de la sécurité juridique, à celle collective.

§.1,1) Le concept de sécurité juridique :

Au sein du principe siègent deux conceptions de la sécurité : la première, sécurité juridique, met l'accent sur le bien personnel de chaque individu, quand la seconde, sécurité collective, renvoie logiquement au bien commun de la société.

La sécurité juridique est traditionnellement fondée sur le contrat social, théorie dégagée par Jean Jacques Rousseau dans son ouvrage majeur[69] : ce dernier fonde l'institution de l'Etat moderne sur un pacte établi entre le pouvoir constituant et le pouvoir constitué, sur la base des principes de liberté, d'égalité et de volonté générale. La liberté personnelle constitue donc l'unique fondement de la sécurité juridique instituée par ce contrat, car elle doit garantir à l'individu la plénitude de l'exercice de ces libertés par l'Etat, sans qu'aucun motif arbitraire ne puisse intervenir pour limiter ces droits et libertés. Cependant, les finalités du contrat social peuvent diverger : ainsi, quand les philosophes John Locke et Jean Jacques Rousseau considèrent que le contrat social vise principalement à garantir l'exercice du droit de propriété, Thomas Hobbes y voit comme première finalité, le rétablissement de la sécurité au travers de sa célèbre formule "*l'homme est un loup pour l'homme*". A ce titre, quand bien même l'auteur du "*Léviathan*" traite de la sécurité personnelle, au sens de la nécessaire préservation de l'intégrité de la personne, le législateur reprend seulement une conception ancienne en affirmant que "*le droit fondamental à la sécurité est à la condition nécessaire à l'exercice des autres liberté(...)*"[70].

[69] ROUSSEAU Jean Jacques, "*Le contrat social*", 1762, Paru chez Marc Michel Rey.
[70] Titre Premier "*Principes généraux de la sécurité intérieure*", Chapitre premier "*Sécurité publique*", Article L.111-1 du Code de la sécurité intérieure de 2012.

La sécurité juridique, fondée sur le contrat social, visant à assurer l'exercice des droits et libertés au premier rang desquelles figurent le droit à la propriété, ou à la sécurité, a de commun son implication en matière d'égalité : c'est que l'autorité publique dispose d'un pouvoir exercé sur l'ensemble de la population, laquelle est mécaniquement en situation d'égalité dorénavant. Enfin, pour garantir cette sécurité juridique, la solidarité doit jouer : l'ensemble des individus, placés dans une situation d'égalité, assurent solidairement la sécurité juridique, dans le but de garantir dans le présent, sinon préventivement, l'exercice des droits et libertés reconnus à chacun.

§.1,2) Le concept de sécurité collective :

La sécurité collective émerge essentiellement depuis la fin de la Seconde Guerre Mondiale, et trouve à s'épanouir dans les contextes de décolonisation, ou de lutte contre la "*néo-colonisation*". Le principe de sécurité collective repose non plus sur un contrat social, mais sur un Pacte des Nations[71] : à ce titre, le premier des droits garanti est aux mains, non plus de l'individu, mais du peuple pour pallier aux risques présents, ou à venir. On parle ainsi de droit des peuples à disposer d'eux-mêmes, ou de droit à être indépendant. Pour l'avenir, on parle de droit au développement durable visant à préserver les ressources disponibles pour les générations actuelles et à venir. La finalité poursuivie sera donc de conserver l'intégrité territoriale, qu'elle soit régionale ou globale, tandis que l'ensemble des Nations seront dans une situation d'égalité souveraine. Enfin, là encore la solidarité joue : elle prend cependant la forme de mécanismes de secours et d'entraide collective cette fois.

§.2/ La sécurité en tant que devoir à la charge des autorités : de la sécurité policière, à celle militaire.

La sécurité ne constitue pas seulement un droit, mais peut constituer aussi un devoir : néanmoins, ce devoir n'est à la charge que des personnes disposant du "*monopole de la violence légitime*"[72]. A ce titre, la sécurité renvoie à celle essentiellement policière et, ou militaire. Cependant, on distingue plusieurs formes de sécurité siégeant dans ces deux catégories : au sein de la sécurité policière, on distingue ainsi la police générale, politique ou totalitaire.

§.2,1) La sécurité policière : versant général, politique, totalitaire.

Concernant la police générale, la sécurité aura pour principale base la conservation des biens et des personnes, elle trouvera à s'exprimer par la réglementation, et privilégiera la surveillance. La finalité poursuivie par la police générale est la conservation de l'ordre public, donc plus prosaïquement la normalité,

[71] On peut prendre comme exemple le Pacte des Nations-Unies de 1945
[72] WEBER Max, "*Le savant et le politique* », Paris : Union Générale d'Editions, 1919

par la prévention de la déviance. Enfin, à l'inverse des concepts de sécurité juridique, celui policier reposera non plus sur la solidarité, mais plutôt sur la délation.

D'autre part, on retrouve le concept en matière de police politique : la préservation de l'ordre public constituera ici non plus le premier objectif, mais bien le fondement de la sécurité policière. Le premier objectif sera quant à lui la préservation de l'état d'exception. La finalité poursuivie par cette police est d'assurer le maintien de l'ordre global, notamment par le biais du renseignement ; elle implique non plus la normalité, mais bien plus la loyauté et repose moins sur la délation, que sur la dénonciation.

Dernier modèle de sécurité policière, celle totalitaire : son fondement sera ici la poursuite du mouvement, quand le premier des droits promus sera la mobilisation afin d'encourager la participation à la cause. Cette police reposera moins sur la surveillance, que sur la vérification. Elle attachera d'ailleurs moins d'importance à la loyauté, qu'au conformisme : elle fonctionne sur le signalement et, ou l'aveu[73].

§.2,2) La sécurité militaire :

La sécurité militaire joue dans le modèle classique "*Westphalien*" : le premier des droits garanti est le droit à la guerre, appelé "*jus ad bellum*", quand les objectifs à poursuivis tiennent à la protection d'intérêts d'Etats : dans cette logique, l'ensemble du système repose sur la "*raison d'Etat*", quand la finalité poursuivie vise à garantir l'équilibre des puissances. Ce modèle est d'ailleurs transposable dans le contexte de guerre froide, et fonctionne alors sur un modèle de bipolarité et de dissuasion. Le premier des objectifs asservi tend à garantir les sphères d'influences respectives, quand l'ensemble est fondé l'alignement idéologique. L'exercice de cette police viendra garantir l'équilibre des menaces, tout en privilégiant le principe d'indiscutable. (*Pour un tableau schématique de ces différents modèles de police contemporaine, se reporter à l'annexe II.)*

Section II/ La construction du droit à la sécurité

Le principe de sécurité a été transposé au niveau national en tant qu'outil du débat démocratique, bien de communication politique (*Sous-section 1*) : il a mécaniquement influencé le législateur à prendre des mesures propres à en assurer l'exercice sur le terrain juridique (*Sous-section 2*)

§.1/ La sécurité dans le langage politique, outil de communication privilégié :

Si le principe contemporain de sécurité a toujours constitué un point de clivage entre les deux principales formations politiques françaises, la première revendiquant le monopole de l'ordre et de la fermeté en matière

[73] Voir le film "*l'aveu*", Costa Gavras, 1970 pour une description de ce régime totalitaire fonctionnant sur l'aveu.

de sécurité, alors que la seconde insistait sur les libertés ; la question de la "*sécurité*" au cœur du débat politique à droite, comme à gauche, fait consensus à la fin des années 1980, période charnière ou culmine le problème de la violence en France comme ailleurs[74] :

Dans un premier temps, se développe une approche globalisante de la "*question de la ville*" impliquant rénovation du bâti, développement social, insertion des jeunes et prévention de la délinquance. Néanmoins, au début des années 1990, le curseur sera progressivement mis sur la question générale de la "*sécurité*" en tant qu'objectif principal. A la fin des années 1990, le point d'orgue de la lutte contre l'insécurité émerge : dans sa déclaration de politique générale du 19 juin 1997, le Premier ministre fait ainsi de la sécurité une priorité gouvernementale et officialise une nouvelle doctrine politique, en proclamant que la "*sécurité*" est au rang de "*première des libertés*", qu'elle est l'enjeu de l'égalité républicaine. Il ne s'agit plus de concilier deux impératifs caractéristiques de chacune des deux formations politiques, à savoir la sécurité pour la droite, et la liberté pour la gauche, mais bien plutôt d'affirmer que la jouissance des libertés ne peut être assurée que lorsque la sécurité est garantie[75].

A ce titre, le colloque de Villepinte "*Des villes sûres pour des citoyens libres*" marque la priorité accordée au programme politique du gouvernement de l'époque : la sécurité doit être garantie au niveau local[76], nécessitant que soient prises de nouvelles initiatives en la matière[77] : dorénavant, "*la sécurité [devient] l'affaire de tous, [...] et ne saurait plus être l'affaire des seules forces de police ni du ministère de l'Intérieur.*"[78]. Progressivement, la sécurité va constituer un bien politique et va recouvrir des catégories générales d'appréhension : le thème de l'"*insécurité*" va ainsi constituer une catégorie "*sui generis*" du débat politique contemporain[79], lequel aura nécessairement sa place à occuper dans le domaine de l'utilisation des technologies numériques. (<u>*Pour plus d'éclaircissements, voir l'entretien réalisé avec M.Bonelli Laurent en annexe I*</u>).

---

[74] A cette époque, Mr.GIULIANI, le maire de New-York, met d'ailleurs en pratique la théorie du "*carreau cassé*" ("*Broken window*"), transposée en France sous le nom de politique de "t*olérance zéro*".
Voir le film "*A most violent year*", réalisé par J.C Chandor, sorti en 2014 illustrant l'atmosphère régnant à New-York en 1981.

[75] Voir sur la question BONELLI Laurent, "*La France a peur. Histoire sociale de l'"insécurité"*, éditions « *La découverte* », 2013, p.67 et ss.

[76] L'article L.2212-2 du Code Général des Collectivités Territoriales (CGCT) prévoit que le maire est chargé d'assurer "*le bon ordre, la sécurité, la sûreté et la salubrité publique*".

[77] Dans cette logique, de nouvelles procédures contractuelles formant la base de la réforme du service public de sécurité vont émerger : il s'agit des Contrats Locaux de Sécurité (CLS) visant à organiser la coproduction de sécurité entre collectivités locales, services déconcentrés de l'Etat, bailleurs sociaux, transporteurs publics, ou la population par exemple.

[78] "*Des villes sûres pour des citoyens libres*", actes du colloque, Villepinte, 24 et 25 octobre 1997, Editions SIRP, pp.3.-4

[79] Concernant l'ensemble des questions écrites, orales et au Gouvernement posées à l'Assemblée nationale durant les trois législatures qui couvrent la période 1988 - 2002, on observe une nette progression du nombre de questions afférentes à la sécurité : si 86 questions portaient sur la "*délinquance juvénile*" pour la onzième législature (1997-2002) contre 5 pour la neuvième (1988-1993), on recense parallèlement 155 questions désormais sur la "*délinquance des mineurs*" contre seulement une question et 1099 questions sur la "*délinquance*" contre 592 durant ces mêmes législatures

§.2/ *La sécurité dans le langage juridique, d'une doctrine politique au droit :*

Si l'on retrouve pour la première fois la notion de "*droit à la sécurité*" dans le langage juridique dans la Déclaration universelle des droits de l'Homme de 1948[1], c'est dans le contexte politique des années 1990, notamment depuis la loi du 21 janvier 1995 relative à la vidéosurveillance[12] que l'on retrouve réellement la notion juridique de "*droit à la sécurité*" en France (*Sous-section I*). De nouvelles questions relatives au modèle de société moderne émergent alors, entre « *société de surveillance* » et « *société de contrôle* » (*Sous-section II*).

§.2.1) Le droit à la sécurité : principe juridique ancré dans le droit français.

L'article premier de la loi du 21 janvier 1995 dispose que "*la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives*": la sécurité en tant que droit fondamental implique non seulement que l'Etat assure son exécution, mais plus encore veille, "*sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens*[80]". La sécurité constitue autant un droit personnel et, ou collectif, qu'un devoir à la charge des autorités publiques.

Par la suite, la loi du 15 novembre 2001 sur la sécurité quotidienne va venir réaffirmer le caractère fondamental du droit à la sécurité, condition *sine qua non* de l'exercice des libertés individuelle et collectives, mais ajoute plus encore qu'elle est la condition de réduction des inégalités, avant que la loi du 18 mars 2003 ne supprime cette dernière mention, sans pour autant dénier le caractère fondamental de ce droit.

Il faudra attendre le 12 mars 2012 pour que soit créé le code de la sécurité intérieure, pris par ordonnance sur le fondement de la Loi d'Orientation de Performance et de Programmation pour la Sécurité Intérieure du 14 mars 2011 (LOPPSI II), pour que les trois proclamations du droit fondamental à la sécurité soit codifiées[81] : en moins de dix ans, il n'est ainsi pas moins question de trois réaffirmations du « *droit fondamental la sécurité* », comme de sa codification en matière de principes généraux de sécurité intérieure.

§.2.2) La sécurité, outil de protection ou de surveillance ?

L'article 17 de la loi LOPPSI II est venu remplacer, dans tous les textes législatifs et réglementaires, le mot "*vidéosurveillance*" par le mot "*vidéo-protection*": la gestion de la sécurité au plan local est passée de l'existant, la vidéosurveillance comme système de constatation des infractions appelant une réaction, à l'objectif : la vidéo-protection. On parle dorénavant d'un "*système d'anticipation des infractions répondant à*

[80] *Ibidem*...

[81] Article L.111-1 du Code de la sécurité intérieure.

une logique de pro-action.[Alors qu'auparavant], l'installation des premiers dispositifs de vidéosurveillance correspondait seulement à une réponse sécuritaire sans intégrer à proprement parler de stratégie d'action(...)"[82]. Par la suite, la vidéo-protection va prendre en compte la mobilité des actes délinquants, et inscrit la politique locale non plus dans une logique de surveillance, mais bien de protection, sinon de contrôle. C'est dire que si les objets utilisés demeurent similaires (caméras de surveillance), leur logique d'utilisation conduit aujourd'hui à parler de garantie de sécurité plutôt que de sûreté des citoyens, comme elle permet enfin de persuader la population qu'il ne s'agit plus seulement de surveiller son comportement, pour mieux contrôler son action, sinon d'assurer sa protection, pour asseoir la nécessité des impératifs de sécurité.

Le fonctionnement de la sécurité sur le plan national passe donc d'un système classique de surveillance, hérité de la tradition de Bentham ou de Foucault[83], au système de contrôle théorisé par le philosophe Gilles Deleuze[84], lequel trouve en particulier matière à s'épanouir sur le terrain numérique au regard notamment des textes de lois relatifs au renseignement en cette année 2015[85]

Section III/ L'émergence d'un nouveau droit fondamental ?

Bien qu'il s'agisse d'un "*droit fondamental à la sécurité*", cette consécration infra-législative ne semble pas conférer au droit une réelle "*fondamentalité*" (*Sous-section 1*) ; cependant, certains textes juridiques invitent à s'interroger sur l'actualité du droit fondamental à la « *sûreté numérique* », lequel a traditionnellement valeur supra-législative (*Sous-section 2*).

§.1/ Quelle réalité du "droit fondamental à la sécurité" ?

Le droit à la sécurité n'est pas apparu de façon autonome, comme vu précédemment il fût accompagné du substantif "*fondamental*" : cependant, peut-on réellement parler d'un droit fondamental à la sécurité ?

Les droits fondamentaux ont progressivement remplacé l'expression de liberté publique dans une nouvelle logique d'approche des « *droits et libertés fondamentaux* » visant à homogénéiser un ensemble. L'expression « *droits fondamentaux* » vise aujourd'hui plus à garantir la protection de l'ensemble contre l'ingérence des autorités publiques, qu'à distinguer ceux des droits exigibles, impliquant une action des pouvoirs publics, des

[82] DECARGUES Géraldine, Directeur de police municipale d'Asnières-sur-Seine.
[83] Le modèle panoptique imaginé par le philosophe BENTHAM Jeremy, décrit dans l'ouvrage "*Surveiller et punir*" de FOUCAULT Michel, 1975, Editions Gallimard, 280 pages.
[84] DELEUZE Gilles, "*Post-scriptum sur les sociétés de contrôle"*, paru dans l'*Autre journal",* mai 1990 ; https://infokiosques.net/spip.php?article214
[85] Voir *infra* Partie II.

libertés nécessitant cette fois une abstention de ces autorités dans leur sphère d'exercice par les citoyens[86] : dans cette logique, le « *droit fondamental à la sécurité* » impliquerait non seulement que les pouvoirs publics ne puissent pas commettre d'ingérence dans les droits des citoyens, mais nécessiterait encore que l'Etat remplisse son devoir d'assurer le droit[87] . On serait donc en présence d'un droit à caractère subjectif d'une part, revêtant le caractère de créance exigible par le particulier envers les pouvoirs publics, comme d'un droit à caractère objectif d'autre part, impliquant le devoir de l'Etat débiteur d'un droit envers le particulier.

Par ailleurs, si on entend par "*droits fondamentaux*" une protection à un niveau « *supra législatif* » des droits et libertés, notamment constitutionnel[88], le droit à la sécurité ne dispose que d'une valeur législative, bien qu'il ait été qualifié de fondamental par certains textes législatifs : c'est dire qu'il s'agit plus de la « *fondamentalité* » contextuelle d'un certain droit[89], que du caractère fondamental d'un droit appelant des évolutions juridiques structurelles.

D'ailleurs, le Conseil d'Etat rappelle que le droit à la sécurité n'est pas une liberté fondamentale au sens du référé-liberté[90] dans son ordonnance du 20 juillet 2001, « *Commune de Mandelieu-La-Napoule* »[91].

Cependant, il est question aujourd'hui des profondes modifications entraîné par le numérique sur le "*régime juridique de plusieurs libertés fondamentales*"[92], parmi lesquelles siègent les nouvelles garanties devant être assurée pour l'exercice de la liberté personnelle[93] face aux nouveaux instruments du droit à la sécurité. Bien que la liberté individuelle, correspondant au droit ne pas faire l'objet d'une détention arbitraire garanti par l'article 66 de la Constitution, se distingue de la liberté personnelle, proclamée par l'article 2 de la Déclaration des Droits de l'Homme du Citoyen de 1789, l'utilisation du numérique à des fins de protection de la sécurité peut aujourd'hui conduire à « *porter atteinte à la liberté personnelle*[94] ».

---

[86] REDOR Marie-Joëlle, « *Garantie juridictionnelle et droits fondamentaux* », Cahier de la recherche sur les droits fondamentaux, n°1, 2002, p.92

[87] L'article premier de la loi du 21 janvier 1995, codifié à l'article L.111-1 du code de la sécurité intérieure prévoit le devoir pour l'Etat d' « *assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, la protection des personnes et des biens* »

[88] FAVOREU Louis, « *Droits et libertés fondamentaux* », Précis Dalloz, 4eme édition, 2007, Paris, p.70

[89] Voir *infra* … Titre 1, Chapitre I, Section II.
Voir annexe I, entretien avec M.BONELLI Laurent.

[90] Article L521-2 du code de justice administrative : « *saisi d'une demande en ce sens justifiée par l'urgence, le juge des référés peut ordonner toutes mesures nécessaires à la sauvegarde d'une liberté fondamentale à laquelle une personne morale de droit public ou un organisme de droit privé chargé de la gestion d'un service public aurait porté, dans l'exercice de l'un de ses pouvoirs, une atteinte grave et manifestement illégale (..)* »

[91] « *Si l'autorité administrative a pour obligation d'assurer la sécurité publique, la méconnaissance de cette obligation ne constitue pas, par elle-même une atteinte grave à une liberté fondamentale au sens de l'article 521-1 du code de justice administrative.* »

[92] *Op.Cit*…« *numérique et droit fondamentaux* »*Ibidem*…, 2014, p.97 et ss.

[93] La liberté personnelle couvre le droit à la vie privée, l'inviolabilité du domicile, la liberté d'aller et venir, la liberté du mariage. Elle est proclamée par l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen de 1789.

[94] *Ibidem*…p.110 et ss.

Ainsi, « *tandis qu'une confusion s'est installée entre la sûreté telle qu'elle figure dans la Déclaration des Droits de l'Homme et du Citoyen de 1789, et la sécurité des personnes et des biens* [95]», il est aujourd'hui encore plus complexe de déterminer si le droit à la sécurité correspond à la protection de la vie privée, ou à la sauvegarde de l'ordre public impliquant protection de l'intégrité des biens et des personnes, et sûreté de ces derniers.

§.2/ Quel avenir pour le "droit à la sûreté numérique" ?

Parallèlement, la Loi LOPPSI II du 14 mars 2011 fixait de nouveaux objectifs en matière de lutte contre la « *cyber criminalité* », et créait le délit d'usurpation d'identité numérique[96] :

Avant l'entrée en vigueur de la loi, la victime de l'usurpation ne pouvait poursuivre l'auteur de l'infraction que si cette usurpation avait constitué le moyen de commettre une infraction au principal comme l'escroquerie, ou l'atteinte à la vie privée et au droit à l'image. Cette nouvelle loi consacre désormais le caractère autonome du délit d'usurpation de l'identité numérique, lequel devient une infraction au principal : ce délit est ainsi consommé lorsqu'il porte sur l'identité même de la victime[97]. Par la suite, l'infraction doit avoir pour but de créer un préjudice effectif ou éventuel résultant du troublé porté à la tranquillité d'une victime directement lésée, ou bien à celle d'un tiers par le biais de l'usurpation d'identité d'une victime au principal, laquelle constitue alors un simple moyen de commettre l'infraction.

Le délit concerne donc deux catégories de victimes : la personne dont l'identité a été usurpée d'une part, ce qui implique que l'infracteur nuise directement à l'image de l'intéressé, à sa réputation et trouble ainsi sa tranquillité ; le tiers trompé d'autre part, ou l'infracteur va induire l'internaute en erreur et lui soutirer des informations et, ou de l'argent. L'usurpation d'identité numérique devient donc soit l'objet même de l'infraction, soit le moyen de commettre une infraction contre un tiers.

Pour parer à ces nouvelles menaces, le législateur a d'ailleurs pu prendre une année plus tard la loi relative à la protection de l'identité numérique[98], appelant à repenser le concept traditionnel de « *sûreté* » sur le terrain numérique. Aujourd'hui, s'il reste prudent de distinguer « *sécurité* » et « *sûreté* », on peut penser que le droit à la « *sûreté numérique* » permet d'assurer la sécurité juridique personnelle des internautes, et tend à consti-

[95] BADINTER Robert, « *Compte rendu intégral des débats du Sénat* », séance du 20 janvier 2004.
[96] Article 226-4-1 du code pénal : « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à s considération, est puni d'un an d'emprisonnement et de 15 000euros d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.* »
[97] Identité numérique comprend alors non seulement le nom, mais aussi le prénom, le surnom, le pseudonyme ou les identifiants électroniques, adresses IP, mots de passe, images voire les avatars lorsque le délit survient dans les réseaux de communication au public en ligne.
[98] Loi du 27 mars 2012 relative à la protection de l'identité numérique.

tuer un droit fondamental à part entière, tandis que le droit à la sécurité viserait plutôt à asseoir une certaine régulation de l'activité, un cohérence d'un ensemble de droits personnels sur le terrain numérique.

Chapitre II :

Le droit à la sécurité confronté au numérique, ou la « *cyber sécurité* »

La "*cyber sécurité*", si elle trouve à s'exercer sur le nouveau terrain numérique (***Section 1***), ne fait pas obstacle à la commission d'infractions classiques (***Section 2*****),** non plus qu'à l'émergence de nouveaux acteurs, autres que les gouvernements : surtout, si elle constitue à l'origine le fruit d'une sécurité militaire, elle permet aujourd'hui d'alimenter le principe de sécurité juridique, comme policière sur le terrain numérique (***Section 3***).

Section I/ La notion de « cyber sécurité » ?

La « *cyber sécurité* », née dans un contexte de guerre froide, résulte directement du concept de sécurité militaire (*Sous-section 1*) : si elle n'est plus de l'apanage des seules autorités militaires, elle nécessite encore aujourd'hui le suivi d'un contrôle dans la sphère publique (*Sous-section 2*).

§.1/ La « cyber sécurité », un outil militaire :

Le néologisme « *cybernétique* »[99] revient à Norbert Wiener[100], il désigne le « *champ entier de la théorie de la commande et de la communication, tant dans la machine que dans l'animal »*. Par la suite, c'est dans la fiction que le terme cyberespace est utilisé, notamment dans la trilogie romancière le « *Neuromancien* »[101] : le personnage principal est alors un voleur de données en mesure d'établir des connexions entre son esprit et un réseau mondial reliant entre eux des ordinateurs[102].

Par-delà ces créations intellectuelles et artistiques, le préfixe « *cyber* » va participer depuis sa création à la construction de nouveaux substantifs relatifs à la société de l'information ayant vu le jour à compter de la fin du XXème siècle[103], quand la « *cyber sécurité* » s'efforcera principalement de permettre à tout internaute de naviguer dans ce cyberespace en toute quiétude. Or, si on pourrait croire que l'exigence de sécurité s'est

[99] Le néologisme « *Cybernétique* » est tiré du grec « *kurbeneïn* », signifiant diriger.
[100] WIENER Norbert, « *Cybernetics* », Paris, Hermann, 1948
[101] GIBSON William, « *Le neuromancien* », Edition Ace Books, 1984.
[102] On retrouve cette idée dans le film « *Transcendance* », réalisé par Wally Pfister, 2014.
[103] ARPAGIAN Nicolas, « La *cyber sécurité* », Que sais-je, PUF, 2010

progressivement imposée postérieurement à la création du cyberespace, il est nécessaire de rappeler que l'exigence de sécurité est plutôt à l'origine de la création du réseau Internet.

Le réseau puise avant tout son origine dans le souhait exprimé dès 1962 par les autorités états-uniennes, notamment l' « *Advanced Research Project Agency* » (ARPA) de disposer d'un système de communication qui résisterait à une attaque nucléaire massive émanant de l'Union soviétique[104]. Faisant écho à ce souhait exprimé par l'ARPA, l'Université de Californie-Los Angeles (UCLA) va élaborer à partir de 1969 le réseau « *Arpanet* »[105].

En France c'est l'ingénieur en informatique Louis Pouzin qui pilote le projet "*Cyclades*", qui va relier 25 ordinateurs installés sur le territoire national, en Italie et au Royaume-Uni afin de permettre aux chercheurs de collaborer à distance en 1971, avant que le projet ne soit finalement abandonné dès 1979[106] : le réseau présentait alors l'avantage de prendre la forme d'une toile d'araignée qui, ne disposant pas de point central, permettait de continuer à faire circuler l'information quand bien même il serait partiellement détruit, ce qui dans les circonstances de l'époque permettrait aux autorités étatsuniennes de survivre à une attaque soviétique : c'est dire que la sécurité a présidé à l'invention d'Internet dans le contexte de guerre froide, que le réseau est avant tout une innovation de la sécurité militaire (*Voir tableau synthétique des concepts de sécurité en annexe II*).

§.2/ « La cyber sécurité », un outil de contrôle :

Pour assurer la pérennité de ce nouvel outil, les Etats ont par la suite été amenés à exercer un contrôle sur le réseau qui, s'il était utilisé en 1996 par 36 millions d'internautes, est aujourd'hui utilisé par 3 milliards d'internautes[107]. La croissance exponentielle de l'utilisation du réseau Internet incite donc rapidement les Etats à opter pour des dispositifs de contrôle et, ou de filtrage des communications numériques pour anticiper des agressions potentielles, ou pour agresser des adversaires[108]. Contrôle d'autant plus important qu'aujourd'hui le cœur de l'économie numérique représente 5,2% du Produit Intérieur Brut (PIB), et 3,7% de l'emploi, tandis que les secteurs peu ou pas touchés par le processus de numérisation ne représentent

[104] COBAST Eric "*Cent jour de mémoire ou d'oubli, les 100 dates de la culture générale*", Collection "Que sais-je", Editions Presses Universitaires de France, date : 1969, p.119
[105] Réseau Arpanet : réseau décentralisé reliant quatre grands centres universitaires américains. Le réseau devient par la suite un réseau mondial d'ordinateurs permettant aux utilisateurs de communiquer (courrier électronique), publier des informations (Web), transférer des données (FTP), travailler à distance (SSH) ou encore de discuter (MSN)
(COBAST Eric « *Les 100 dates de la Culture Générale* », Collection « *Que Sais-Je ?* », Editions « PUF », 2010.)
[106] ARPAGIAN Nicolas, « La *cyber sécurité* », Collection « Que Sais-Je ? », Editions PUF, 2010, p.9 et ss.
[107] Conseil d'Etat, section du rapport et des études ; données : « *Internet World Stats et International Telecommunication Union* », Etude annuelle, Conseil d'Etat, « *le numérique et les droits fondamentaux* », 2014 p.43
[108] *Op.Cit…."La cyber sécurité" Ibidem*…. p.13 et ss.

qu'un peu plus de 22% du PIB[109] : la survie de la Nation passe ainsi par la prévention des attaques extérieures contre le réseau, la sécurité intérieure par le maintien de fonctionnement du réseau.

Aujourd'hui, la « *cyber-sécurité* » constitue donc moins un outil au service de la sécurité militaire, qu'un outil de surveillance, sinon de contrôle[110] au service d'une police générale dans nos sociétés contemporaines. (*Voir tableau en annexe II pour un schéma explicatif des différents modèles contemporains de police*).

Section II/ Les atteintes classiques à la « cyber sécurité »

Si les attaques commises dans le cyberespace convergent dans les réseaux informatiques et téléphoniques, leur destination diverge quant à la cible à atteindre : le réseau constitue respectivement la cible directe de l'attaque (*Sous-section 1*), ou l'intermédiaire nécessaire à la réalisation de l'attaque (*Sous-section 2*).

§.1/ Le réseau, cible directe de l'attaque informatique :

Les attaques directes contre les systèmes informatiques visent à accéder à des données confidentielles, à détruire ou altérer des données, à entraver enfin le bon fonctionnement du système ou utiliser des ressources informatiques à l'insu de leur détenteur. Elles se commettent par le biais de différents procédés informatiques, parmi lesquels figurent les virus, les vers, les chevaux de Troie, ou encore les attaques par refus de service[111].

Ces attaques sont généralement commises par différents acteurs : ceux-ci peuvent être des individus isolés, des organisations criminelles, des entreprises ou même des Etats. Le développement de l'Internet mobile, l'interconnexion des terminaux, la dépendance de plus en plus croissante des particuliers, entreprises, administrations d'Etat aux technologies numériques nécessite de considérer sérieusement ces attaques. A cet égard, le législateur[112] a défini dès 1988 les infractions spécifiques pour punir ce genre d'atteintes au « *système de traitement automatisé de données* » (STAD) : les articles 323-1 à -7 du code pénal incriminent dorénavant « *l'accès frauduleux à un STAD, l'entrave à leur fonctionnement, ou encore la modification ou la suppression frauduleuse de données* », quand la peine peut aller jusqu'à deux ans d'emprisonnement et 30 000euros d'amende lorsqu'il est question d' « *accès frauduleux* », jusqu' à cinq ans d'emprisonnement et

[109] Inspection générale des finances, *« Le soutien à l'économie numérique et à l'innovation* », rapport n°2011-M-060-02, janvier 2012, p.21
[110] Voir *infra*…. Partie II, Titre II, Chapitre I
[111] *Op.Cit …* « *numérique et les droits fondamentaux* », *Ibidem*…. p.122 et suivantes pour des définitions synthétiques de ces différents procédés.
[112] Loi « *Godfrain* » du 5 janvier 1988 relative à la fraude informatique.

75 000euros d'amende lorsqu'il est question en plus d' « *entrave, d'introduction frauduleuse de données* » depuis 2012[113].

Plus récemment, c'est loi relative à la lutte contre le terrorisme sur le terrain numérique du 13 novembre 2014 qui prévoit que lorsque ces infractions [au STAD] sont commises en bande organisée, la peine est alors portée à dix ans d'emprisonnement et à 150 000euros d'amende (article 323-4-1 du code pénal) : il s'agit dès lors de développer en premier lieu la protection de la sécurité juridique des internautes sur le terrain numérique, de prévenir les atteintes commises à l'encontre de la Nation.

§.2/ Le réseau, intermédiaire nécessaire à la réalisation de l'attaque :

Comme le souligne le rapport du Conseil d'Etat de 2014, « *le numérique n'est pas à l'origine de formes de délinquance telles que la contrefaçon, l'escroquerie ou la pédophilie, [cependant] il les facilite et en fait apparaître de nouvelles formes* »[114]. Parmi ces nouvelles formes de délinquance figurent non seulement le délit d'usurpation d'identité[115], mais aussi l'atteinte au droit de la propriété intellectuelle.

Le champ d'action de ce dernier droit a logiquement été étendu aux œuvres numériques, comprenant les logiciels et bases de données, comme aux usages numériques des œuvres culturelles, comprenant cette fois la numérisation des œuvres et leur diffusion sur Internet. Le législateur a ainsi inclut dès 1985[116] les logiciels dans la liste des œuvres protégées par le droit d'auteur : or, si le droit d'auteur confère à son titulaire un droit de représentation, consistant en « *la communication de l'œuvre au public par un procédé quelconque* [117]», et le droit de reproduction, recouvrant cette fois *« la fixation matérielle de l'œuvre par tous procédés qui permettent de la communiquer au public d'une manière indirecte*[118] », les œuvres numériques et le procédé de diffusion sur Internet se heurtent aujourd'hui aux dispositions de ces deux droits. Ainsi, la numérisation d'œuvres et leur mise à disposition sans consentement préalable des titulaires de ces deux droits peuvent constituer un acte de contrefaçon[119] : c'est ainsi le droit de propriété qui est sauvegardé, le principe à la base du contrat social entre l'individu et l'Etat venant instaurer la sécurité juridique qui est préservé.

[113] Loi du 27 mars 2012 relative à la protection de l'identité.
[114] *Op. Cit* … « *Le numérique et les droits fondamentaux* » *Ibidem*…. Pages 115 et ss.
[115] Voir *infra* …Partie I, Titre II, Section III, Sous-section 2
[116] Loi du 3 juillet 1985.
[117] Article L.122-2 du Code de propriété intellectuelle.
[118] Article L.122-3 du Code de propriété intellectuelle.
[119] *Op.Cit…* « *le numérique et les droits fondamentaux* » *Ibidem*… p.126 et ss.

Section III/ Les acteurs de la « cyber-sécurité »?

La « *cyber sécurité* » n'est plus de l'apanage des seuls gouvernements, ni des armées régulières : elle fédère aujourd'hui moins les organisations internationales intergouvernementales, que celles non gouvernementales (*Sous-section 1*), les entreprises ou les particuliers : à ce titre, elle consacre l'exercice d'une sécurité collective aujourd'hui (*Sous-section 2*).

§.1/ Organisations internationales :

§.1.1/ Organisations intergouvernementales :

Les organisations intergouvernementales essaient essentiellement de répondre à des enjeux d'avenir liés l'utilisation du numérique : elles sont principalement au nombre de six[120].

L'Organisation des Nations Unies (ONU), a l'instar des sommets de Kyoto et de Rio sur l'environnement, a jugé qu'Internet méritait une rencontre solennelle des chefs d'Etat et de gouvernement : à ce titre, une première rencontre s'est tenue à Genève en décembre 2003 afin de traiter d'un premier volet relatif à la société de l'information[121] organisé par l'agence spéciale[122] de l'ONU dans ce domaine ; le second volet se tint quant à lui à Tunis, en novembre 2005 et a conduit à constituer un Forum sur la gouvernance de l'Internet[123]. Ces deux sommets n'ont cependant pas constitué des lieux des prises de décisions immédiates, mais ont plutôt constitué des terrains d'influence, de réflexion comportant de nombreux groupes de travail et des réunions plénières.

Le G8[124] a appréhendé quant à lui les problématiques sécuritaires liées à l'usage de l'Internet dès la fin des années 1990 : lors d'une rencontre des ministres de l'Intérieur et de la Justice le 9 et le 10 décembre 1997, les participants ont mis en place un réseau de correspondants « *High Tech Crime Point of Contact Network »*, appelé plus simplement « *24/7 »*[125]. Cependant, cette lucidité se heurte aujourd'hui à des contraintes techniques, tandis que la coopération internationale bute sur les divergences juridiques des droits nationaux face à une criminalité naturellement mondialisée : c'est que l'union ne fait pas toujours la force, et peut même constituer une faiblesse.

L'OCDE a eu de commun avec le G8 sa clairvoyance précoce concernant les problématiques liées à l'usage d'Internet : inquiétée depuis les années 1970 de la possible exploitation malintentionnée des données pri-

---

[120] Organisation des Nations Unies (ONU), G8, Organisation de Coopération et Développement Economique (OCDE), Union Européenne (UE), Organisation du Traité de l'Atlantique Nord (OTAN), Interpol.
Op.Cit …« La *cyber sécurité* », *Ibidem*….p.80 et ss.
[121] Compte rendu disponible : www.iut.intl/wsis/index-fr.html
[122] L'Union Internationale des Télécommunications (UIT)
[123] Compte rendu disponible : http:intogvforum.org/cms
[124] Le G8 rassemble rassemblant l'Allemagne, le Canada, les Etats-Unis, la France, l'Italie, le Japon, le Royaume-Uni, la Russie
[125] Les équipes sont à même de communiquer entre elles sept jours sur sept, 24heures sur 24, afin de réagir le plus promptement possible en cas de cyberattaque

vées accumulées par les systèmes informatiques des entreprises, elle dresse des rapports avertissant les autorités politiques chargées de l'économie de ces périls des cyberattaques, et démontre que les logiciels malveillants peuvent constituer une menace mortelle pour l'économie d'Internet en 2008[126]

Au niveau européen, les vingt-huit états membres disposent depuis 2004 d'une Agence Européenne chargée de la Sécurité des Réseaux de l'Information (ENISA) : elle n'a cependant jamais reçu des moyens réels de se développer, ni ceux qui lui permettrait de travailler sur le fond des dossiers qu'elle a à traiter. Basée à Héraklion en Crète, ses maigres financements annuels à hauteur de 8millions d'euros ne lui permettent pas en l'état actuel d'avoir un poids suffisant dans la guerre numérique, tandis qu'elle avait une durée d'existence de seulement cinq ans.

Concernant l'OTAN, c'est au lendemain des cyberattaques menées contre le nouveau membre de l'Organisation en 2007[127] que l'Alliance atlantique a été la première organisation internationale réellement confrontée à la guerre numérique : l'ampleur des attaques menées a d'ailleurs conduit la République balte à invoquer l'article 5 du Traité fondateur de 1949 prévoyant que lorsqu'un membre de l'Alliance est attaqué, celle-ci doit lui venir en aide et participer éventuellement à la riposte, sans que cet article n'ait cependant joué dans cette affaire.

l'Alliance a néanmoins ouvert un centre d'analyse et d'expertise en matière ce « *cyber sécurité* » à Tallin : il s'agit avant tout d'un groupe chargé de réfléchir aux enjeux et perspectives en matière d'attaques numériques auquel seuls sept Etats participent aujourd'hui[128]. La même année fût créée une Autorité politique chargée de la cyberdéfense (CDMA) dont le rôle est de lancer et coordonner des mesures immédiates de cyberdéfense chaque fois que les circonstances l'exigent.

Enfin, face à la montée en puissance de la « *cyber criminalité* » organisée, Interpol s'est dotée en 2008 d'une unité d'informatique légale et dispose de son propre maillage de correspondants internationaux en contact 24heures sur 24 : il s'agit d'une avancée supplémentaire en matière de coopération policière internationale. Cette instance regroupe tous les deux ans une conférence réunissant praticiens, universitaires, juristes et experts techniques du secteur privé afin d'échanger sur les pratiques « *cyber criminelles »* présentes et à venir[129].

[126] Rapport disponible à cette adresse : www://oecd.orf/dataoecd/53/34/40724457.pdf
[127] L'Estonie
[128] Estonie, la Lituanie, la Lettonie, l'Espagne, l'Allemagne, l'Italie et la Slovaquie
[129] *Op.Cit*… « *La cyber sécurité* » *Ibidem*....p.80 et ss.

§.1.2/ Organisations non-gouvernementales :

Un nombre toujours plus important d'associations ou d'organisations non-gouvernementales s'intéressent au phénomène Internet. Les plus emblématiques sont cependant au nombre de trois[130] :

L' « *Internet Corporation for Assigned Names and Numbers »* (ICANN) est une structure de droit privé californien à but non lucratif, elle fonctionne sur un protocole signé avec le ministère du Commerce des Etats-Unis : la structure gère au niveau mondial les noms de domaine. A ce titre, il lui revient d'octroyer aux Etats, entreprises, individus, l'adresse qui leur permettra d'exister sur Internet. Elle est par ailleurs libre de retirer à tout moment cette adresse et rendre un site inaccessible sur le réseau : elle dispose donc d'un pouvoir considérable, et unique sur le globe. A titre d'exemple, il faut attendre le 30 octobre 2009 pour que son directoire vote en faveur de l'enregistrement de noms de domaines en arabe, chinois, coréen et japonais tandis que les populations pratiquant ces langues représentent environ la moitié des 3milliards d'internautes recensés dans le monde.

Le « *World Wide Web Consortium »* (W3C) est un organisme à but non lucratif créé en 1994, visant à assurer l'interopérabilité des différentes technologies qui cohabitent sur Internet. Cet organisme s'appuie sur une collaboration avec des structures comme le MIT, et concentre les principaux centres de recherche informatique de l'Union européenne parmi lesquels figurent par exemple l'Institut National de Recherche en Informatique et en Automatique (INRIA). Le W3C produit des recommandations transmises aux industriels, et reste financée par des dons ou des cotisations privées.

L' « *Internet Engineering Task Force* » (IETF), dont la devise est « *les contributeurs à l'IETF n'aiment guère la bureaucratie !* » permet à chacun de se saisir d'une thématique technique et de commencer à rédiger un « *appel à commentaires* » : le document doit être envoyé sur le site internet de l'IETF et se trouve soumis aux critiques, avis et analyses de la communauté des internautes. Si le document laisse tout le monde indifférent, il devient caduc ; mais s'il suscite des réactions, l'IETF pourra alors constituer un groupe de travail qui lui sera consacré afin que les différents documents finissent par décrire les aspects techniques liés à l'usage d'Internet. Ce mode original de production des différents protocoles sur lesquels repose Internet constitue ainsi un processus sans équivalent dans le monde normatif classique.

[130] *Op.Cit…*« La *cyber sécurité* » *Ibidem….*p.91 et ss.

§.2/ Les entreprises et les particuliers :

§.2.1/ Les entreprises :

Les sociétés commerciales veulent aujourd'hui profiter de la mobilité facilitée par les outils électroniques : la prolifération d'attaques informationnelles, les connexions à distance et les occasions de perte des supports numériques apparaissent cependant comme des risques réels pour leur intégrité. Par ailleurs, si le transfert systématique à des sous-traitants de toute la capacité informatique de la société peut représenter une menace sur la confidentialité des données, la « *cyber sécurité* » joue plus que jamais un rôle majeur dans le monde de l'entreprise[131].

L'étude menée en 2009 par l'Institut National des Statistiques et Etudes Economiques (INSEE), « *l'insécurité numérique des entreprises* » dresse à cet égard un panorama des craintes, et réponses privilégiées par les chefs d'entreprises : quand 43% d'incidents liés à des envois de spams étaient constatés concernant les dirigeants, 53% des chefs d'entreprises admettaient avoir mené une action d'enquête interne à la suite de tout type d'incident, quand seulement 5% préféraient intenter une action en justice. Cette action d'enquête interne est d'ailleurs la plus fréquemment utilisée quand il s'agit de répondre à un incident concernant un non-respect des directives de sécurité (69%), l'existence d'un virus ou d'un ver (63%), de spams (55%) ou une perte de données (58%). Cependant ces divers types d'incidents n'aboutissent que dans 38,5% des cas à une révision de la politique de sécurité de l'entreprise.

Il ressort donc de l'enquête que si la constatation d'incidents informatiques n'est pas généralisée dans les entreprises, la banalisation des réponses sécuritaires informatiques reste privilégiée[132].

§.2.2/ Les particuliers :

L'étude « *Confiance des Français dans le numérique* » menée par la Caisse des dépôts et consignations en mars 2010 recense 68% d'internautes réguliers parmi les utilisateurs d'Internet :

Parmi ces internautes réguliers, 76% se connectent tous les jours et 89% ont déjà effectué une démarche administrative en ligne, enfin 80% consultent leurs comptes bancaires sur Internet : la banalisation de l'usage d'Internet touche ainsi l'ensemble des particuliers, indépendamment de leur niveau d'étude ou des connaissances en informatique. L'étude démontre plus encore que les utilisateurs français d'Internet appréhendent non pas la sécurité par rapport au réseau lui-même, mais bien par rapport à la destination du site consulté : la mesure de sécurité adoptée tient ainsi au changement d'identité numérique chaque fois qu'ils se connectent sur un nouveau site : à ce titre, ils disposent en moyenne de douze comptes en ligne[133]. Concernant la sensi-

[131] Voir à cet égard le dossier « *Cyber-menaces : mythe ou réalité* », troisième partie *« La cyber-résilience des entreprises mis à rude épreuve* » de MEYNET Stephane, GHEMAOUTI Solange, AGHROUM Christian, QUEMENER Myriam, SOUVIRA Anne, revue « *Securité et stratégie* », n°11, décembre 2012 – fèvrier 2013, La Documentation Française.

[132] *Op.Cit…* « La *cyber sécurité* » *Ibidem…* p.87 et ss.

[133] Deux ou trois adresses pour la messagerie instantanée, un ou deux profils pour la messagerie, deux pseudonymes pour les utilisateurs de forums et un compte sur quatre sites de commerce électronique

bilité des informations, 71% des internautes Français considèrent qu'elle concerne avant tout les données sur leur santé, quand respectivement 51% et 49% considèrent que relèvent du domaine des informations sensibles, celles touchant à leur vie personnelle et leur état civil. Cependant, ils sont 94% à ne pas hésiter à communiquer leurs noms et prénoms sur Internet, 82% à communiquer leur numéro de téléphone et 63% à diffuser en ligne leur numéro de carte bancaire[134].

En résumé, comme le souligne Nicolas Arpagian, « (…)*l'individu selon qu'il s'exprime en tant que citoyen, consommateur ou électeur, formulera en matière de « cyber-sécurité » des attentes et exigences diverses, voire contradictoires car il voudra à la fois circuler librement, mais exigera en parallèle la confidentialité de ses informations : la difficulté liée à l'usage d'Internet tient ainsi dans la conciliation entre modèle économique, nécessité de surveillance et droit à la vie privée des utilisateurs* ».

TITRE III / Numérisation des attributs juridiques de la personne

L'émergence des nouvelles technologies du numérique a nécessité le développement d'un régime juridique propre à garantir l'exercice de certains droits classiques dans le cyberespace (**Chapitre I**), comme elle conduit à faire muter (**Chapitre II**), sinon à créer de nouveaux droits fondamentaux contemporains (**Chapitre III**).

Chapitre I :

Régime juridique classique de l'exercice des droits dans l'espace numérique :

La loi "*Informatique et Libertés*" est un outil juridique vivant commun à l'exercice des droits sur Internet (***Section I***), quand la Commission Nationale Informatique et Liberté (CNIL) est le principal acteur chargé de veiller au respect de ces libertés dans le monde numérique (***Section II***)

Section I/ La loi « Informatique et Libertés »

La loi "*Informatique et Libertés*" du 6 janvier 1978, bien que fixant le régime juridique traditionnel relatif à l'exercice des droits des utilisateurs d'Internet (*Sous-section I*), reste avant tout un outil juridique vivant adapté aux actuelles conditions de vie dans nos sociétés numériques : elle constitue aujourd'hui l'instrument classique de protection de la sécurité juridique des internautes (*Sous-section II*).

[134] *Op.Cit*… « *La cyber sécurité* » *Ibidem*…p.87 et ss.

§.1/ Le régime juridique traditionnel fixé par la loi du 6 janvier 1978 :

La loi "*Informatique et Libertés*" du 6 janvier 1978 vient définir les principes généraux à respecter lors de la collecte, du traitement et de la conservation des données personnelles :

A cet égard, cette loi vient renforcer les droits des personnes sur leurs données, prévoit une simplification des formalités administratives déclaratives, précise enfin les pouvoirs de contrôle et de sanction de la CNIL[135]. Cependant, cet instrument législatif est seulement applicable au traitement automatisé, manuel, informatique ou "*papier*" pour autant que ceux-ci contiennent des informations personnelles relatives à des personnes physiques. Sont dont exclus du champ d'application de la loi, les traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles (agendas électroniques, répertoires d'adresses, sites internet familiaux par exemple), comme les personnes morales, sans faire obstacle cependant à l'application de la loi dans les cas ou des noms de personnes physiques figurent dans le fichier[136].

La loi a pour principal objectif d'éviter une informatisation incontrôlée des administrations centrales, et s'intéresse donc plus au fichiers pris dans ce genre d'administrations (traitement automatisé, manuel, informatique ou papier comportant des données personnelles), qu'au traitements pris dans le cadre de relations interpersonnelles (agendas électroniques, répertoires d'adresses) : cet outil juridique vise ainsi à rassurer principalement l'opinion publique concernant les usages rendus possibles par le développement de l'informatique.

Il est d'ailleurs nécessaire de rappeler que cette loi fût pris à la suite de l'affaire SAFARI[137] de 1974, concernant la mise en place le dispositif d'interconnexion de fichiers à l'aide du numéro attribué par l'Institut National des Statistique et Etudes Economiques (INSEE), laquelle présentait un danger pour la protection des données personnelles des utilisateurs, récoltées à leur insu.

Par la suite, la loi a été modifié par plusieurs lois parmi lesquelles figure notamment celle du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[138], marquant ainsi l'objectif prioritaire de protection des données personnelles face au développement des technologies numériques : il s'agit dès lors moins d'assurer une sécurité policière globale de l'activité d'Internet, que de préserver la sécurité juridique des utilisateurs du réseau.

---

[135] Voir *infra*…Partie I, Titre III, Chapitre I, Section II
[136] Correspondant Informatique et Libertés du Centre National de la Recherche Scientifique (CNRS), www.cil.cnrs.fr
[137] SAFARI : "*Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*"
[138] Loi n°2004-801 du 6 août 2004.

§.2/ Un régime actuel consolidé par la loi du 17 mars 2014 :

La loi du 17 mars 2014 relative à la consommation[139] est venue modifier la loi "*Informatique et Libertés*" du 6 janvier 1978 : elle permet notamment à la CNIL d'effectuer des contrôles en ligne et de constater depuis un ordinateur connecté à Internet des manquements à la loi de 1978.

La section III de la loi vient renforcer et harmoniser les pouvoirs et moyens d'action communs à la protection économique du consommateur, à la conformité et à la sécurité des produits à la concurrence : l'article 105 de la loi dispose dorénavant qu'"*en dehors des contrôles sur place et sur convocation, [la CNIL] peut procéder à toute constatation utile [notamment] à partir d'un service de communication au public en ligne, [afin] de consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers*". Enfin, la même autorité peut dorénavant "*(..) déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label (..) et retire le label lorsqu'elle constate, par tout moyen, que les conditions qui ont permis sa délivrance ne sont plus satisfaites*"[140].

S'il était logique que la CNIL se voit attribuer de nouveaux moyens numériques dans sa lutte contre les menaces à l'égard des droits et libertés reconnus sur le terrain de l'Internet, l'érigeant ainsi en gardienne des droits et libertés numériques fondamentaux, la nouveauté réside dans l'élargissement des pouvoirs de cette autorité qui peut dorénavant prétendre aujourd'hui au poste de régulatrice des activités numériques globales.

Section II/ La Commission Nationale Informatique et Liberté (CNIL)

Les dix-sept membres de la CNIL, élus par les assemblées ou juridictions auxquelles ils appartiennent (*Sous-section I)*, sont chargés de veiller à ce que l'informatique ne porte pas atteinte ni à l'identité humaine, ni aux droits de l'homme, aux libertés individuelles ou publiques : à ce titre, ils veillent à garantir la préservation de la dimension humaine dans le réseau, à développer le concept d'une « *sécurité humaine* » sur le terrain numérique (*Sous-section II)*

§.1/ Composition :

La CNIL est avant tout une institution de l'Etat chargée, en son nom, d'assurer la régulation de secteurs considérés comme essentiels et pour lesquels le Gouvernement veut éviter d'intervenir trop directement : c'est qu'il s'agit avant tout de rassurer l'opinion publique concernant l'utilisation qui est faite par les

[139] Loi n°2014-344 du 17 mars 2014 relative à la consommation.

[140] Article 17 de la loi du 17 mars 2014 relative à la consommation.

administrations centrales des informations personnelles récoltées sur le terrain numérique, ce qui exclut *de facto* que l'Etat intervienne en qualité de contrôleur de la propre gestion de ces informations.

La CNIL, en tant qu'autorité administrative indépendante, comprend 12 à 17 membres élus ou désignés par les assemblées ou juridictions auxquelles ils appartiennent : à ce titre, elle concentre des conseillers d'Etat (Isabelle Falque-Pierrotin), des membres de la Cour de cassation (Marie-France Mazars), des membres du Conseil Economique Social et Environnemental (Dominique Castera et Eric Peres), des sénateurs (Loïc Herve) et députés (Philippe Gosselin) ou encore des chercheurs (Maurice Ronai). La CNIL élit son Président parmi ses membres, et ne reçoit aucune instruction d'aucune autre autorité tandis que les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées ne peuvent s'opposer à son action. Par la suite, le Président nommé recrute librement ses collaborateurs, et les agents exerçant leur activité au sein la CNIL auront qualité d'agents contractuels de l'Etat[141].

Bien qu'elle constitue une institution, qui plus est indépendante, les décisions prises par la CNIL peuvent toujours faire l'objet de recours devant la juridiction administrative : c'est à ce titre qu'on parle d'autorité, et non pas d'institution judiciaire.

§.2/ Compétence :

La CNIL exerce plusieurs missions, lesquelles sont axées autour de sept thèmes : informer, protéger, conseiller et réglementer, accompagner la conformité, contrôler, sanctionner et enfin anticiper.

Concernant son premier champ d'action, la CNIL est investie d'une mission générale d'information des personnes des droits que leur reconnaît la loi "*Informatique et Libertés*" : à ce titre, elle répond à leurs demandes, mène des actions de communication, participe à des colloques, salons ou conférences. Fédérant un collectif de 60 organismes menant des actions en faveur de l'éducation au numérique, elle informe les pouvoirs publics et forme des correspondants "*Informatique et Libertés*".

La protection passe par la mise à disposition du dispositif de "*plainte en ligne*"[142] : il vise à permettre la suppression de contenus sur Internet, à s'opposer à recevoir de la publicité ainsi qu'à accéder ou mettre à jour ses données personnelles. Les demandes touchent prioritairement au secteur de l'Internet et des télécoms, et visent principalement les fichiers Systèmes JUdiciaires de Documentation et d'EXploitation (JUDEX) utilisés par les services de police ou gendarmerie nationale[143].

[141] Informations recueillies sur le site de la CNIL : www.cnil.fr
[142] Disponible à cette adresse : http://www.cnil.fr/vos-droits/plainte-en-ligne/
[143] Voir *infra*….Partie II, Titre III, Chapitre II

Le conseil et la réglementation visent à réguler la circulation des données personnelles par des outils d'autorisations de mise en œuvre des traitements. Ce champ d'action recouvre par ailleurs les avis sur des projets de textes d'origine gouvernementale impliquant des données personnelles ou créant de nouveaux fichiers, comme les cadres juridiques simplifiant l'accomplissement de formalités préalables, le recommandations permettant de fixer la doctrine de la CNIL dans certains domaines, les demandes de conseils des responsables de traitement enfin, par le biais des correspondants "*Informatique et Libertés*".

Les correspondants "*Informatique et Libertés*" font notamment partie intégrante de l'accompagnement dans la conformité : ce champ d'action recouvre le développement des labels, les règles internes d'entreprises encadrant le transfert de données multinationales hors Union Européenne, la création de référentiels sectoriels couvrant des secteurs d'activités ou des branches professionnelles dans leur intégralité.

Enfin, dans une logique de contrôle, la CNIL peut accéder à tous les locaux professionnels, demander communication de tout document nécessaire afin d'en prendre copie, ou recueillir tout renseignement utile, accéder enfin aux programmes informatiques et données[144]. Après qu'aient été exercés ces différents pouvoirs, la CNIL peut prendre diverses sanctions à l'égard de responsables de traitements n'ayant pas respecté la loi : les sanctions prennent la forme d'avertissements, de sanctions pécuniaires jusqu'à hauteur de 300.000euros, d'injonction de cesser le traitement, de retrait d'autorisation accordée préalablement par l'institution.

En cas d'urgence et d'atteinte aux droits et libertés, ces sanctions peuvent consister dans le verrouillage des données pour trois mois, ou dans l'interruption de mettre en œuvre le traitement.

Le thème d'action relatif à l'anticipation passera enfin par la prise en compte de nouveaux sujets autour de tendances, technologies ou d'usages émergents, d'incitation au développement des recherches universitaires concernant la protection de la vie privée et des données personnelles (Prix de thèse "*Informatique et Libertés*")[145].

Chapitre II/ Création de nouveaux droits dans l'espace numérique :

Le développement de l'outil Internet a entraîné la reconnaissance de nouveaux droits fondamentaux : il s'agit du "*droit d'accéder à Internet*" (***Section II***), ou du "*droit à la protection des données personnelles*" de l'utilisateur (***Section I***), lequel implique notamment le "*droit à l'oubli*" depuis l'année 2014 : à ce titre, le

[144] Voir *infra* …Partie I, Titre II, Chapitre I, Section I, Sous-section 2
[145] Informations recueillies sur le site de la CNIL : www.cnil.fr

numérique constitue un vecteur de protection de la sécurité juridique des internautes à part entière (***Section III***).

Section I/ Le droit à la protection des données personnelles

Le droit à la protection des données personnelles a été reconnu pour la première fois en droit français par la loi "*Informatique et Liberté*" du 6 janvier 1978, laquelle reconnaît deux catégories de droits : la première recouvrant des droits à caractère subjectif (*Sous-section I*), la seconde renvoyant à des principes objectifs (*Sous-section II*).

§.1/ Première catégorie de droits :

Il s'agit d'une part du droit d'opposition[146] disponible pour les personnes, et visant à ce que des données personnelles ne fassent pas l'objet d'un traitement, excepté lorsque le ce traitement répond à une obligation légale ou lorsque ce droit a été expressément écarté par l'acte autorisant le traitement.

Ce droit d'opposition s'exerce notamment au moment de la collecte d'information, ou au plus tard en s'adressant au responsable du fichier : c'est un droit personnel qui ne peut être étendu aux informations relatives à des tiers ou des membres de la famille de la personne concernée, excepté les cas de représentation de mineurs ou majeurs protégés. Lorsque ce droit joue pour la personne concernée, l'organisme contacté dispose d'un délai de deux mois pour répondre à la demande d'opposition : la réponse n'emporte pas mécaniquement l'accord de l'organisme, et celui-ci peut refuser d'accepter la demande d'opposition, pour peu que ce refus soit justifié par le responsable du traitement, sauf lorsque la demande est manifestement abusive.

En cas d'absence de réponse, emportant refus tacite, la personne peut saisir la CNIL et les tribunaux[147]. Ce droit d'opposition n'existe cependant pas pour de nombreux fichiers du secteur public comme ceux des services fiscaux, des services de police, de justice ou de la sécurité sociale.

Il s'agit aussi du droit d'accès aux informations[148], tendant à déterminer si le traitement comporte des informations personnelles, ce qui implique cas échéant le droit d'en obtenir communication :

---

[146] Article 38 de la loi "*Informatique et Liberté*" du 6 janvier 1978 : "*Toute personne physique a le droit de s'opposer, pour des motifs légitimes à ce que les données de caractère personnel le concernant fassent l'objet d'un traitement.*"

[147] Voir le guide complet sur le droit d'opposition disponible sur le site de la CNIL : www.cnil.fr/vos-droits/exercer-vos-droits/le-droit-dopposition/

[148] L'article 39 "*Informatique et Liberté*" du 6 janvier 1978 : "*Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel* (…)

La personne souhaitant exercer ce droit doit écrire au responsable de fichier pour lui demander de faire parvenir une copie, en langage clair, de l'ensemble des données concernant l'intéressé qui sont à sa disposition, et joint à cet égard une pièce d'identité avec mention des dates et lieux de naissance dans le but de prouver son identité au responsable du fichier. En l'absence de réponse formulée de manière satisfaisante dans un délai de deux mois suivant cette demande, l'intéressé peut alors porter plainte auprès de la CNIL.

Néanmoins, si un responsable de traitement estime que la demande est manifestement abusive, il peut là encore ne pas y donner suite : l'affaire est alors portée devant un juge et la preuve du caractère abusif de la demande sera à la charge du responsable du système de traitement[149].

Enfin, le droit de rectification[150] implique que l'individu puisse exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées des informations le concernant, si celles-ci s'avèrent "*inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite*". L'intéressé devra effectuer les mêmes démarches que pour le droit d'accès aux informations, tandis que le responsable du système de traitement sera soumis aux mêmes obligations précédentes (respect d'un délai de deux mois suivant l'introduction de la demande).

Cependant, là encore ce droit comporte des limites et ne peut s'appliquer aux traitements littéraires, artistiques et journalistique : de plus, si les héritiers d'une personne décédée peuvent exiger du responsable d'un traitement de prendre en considération le décès et, ou de procéder aux mises à jour nécessaires, les fichiers de police, gendarmerie et renseignement excluent tout exercice du droit de rectification[151].

§.2/ Seconde catégorie de droits :

Les droits de seconde catégorie proclamés par la loi "*Informatique et Libertés*" revêtent un caractère plus objectif : ils visent moins à garantir la sécurité personnelle, qu'à proclamer le concept de "*sécurité humaine*"[152] dans le cyberespace.

---

[149] Voir guide de la CNIL concernant l'exercice de ce droit : www.cnil.fr/vos-droits/exercer-vos-droits/le-droit-dacces/

[150] Article 40 de la loi "*Informatique et Libertés*" : *Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement de données que soient, selon le 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."*

[151] *Ibidem*... www.cnil.fr/vos-droits/exercer-vos-droits/le-droit-de-rectification/

[152] La doctrine de la "*sécurité humaine*" signifie la "*protection des individus contre les menaces, qu'elles s'accompagnent ou non de violence, vise à protéger le noyau vital de toutes les vies humaines, d'une façon qui améliore l'exercice des libertés et facilité l'épanouissement humain*" (Rapport de la Commission sur la sécurité humaine de 2003)

On retrouve ces droits aux premiers articles de la loi, qui posent et déterminent les lignes conductrices concernant l'utilisation de l'informatique face aux libertés. Ainsi, l'article 1er de la loi dispose que "*l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne droit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*". Par la suite, les articles 2 et 3 vont préciser les champs d'application de la loi, notamment en précisant qu'elle s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans ces fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles[153].

Les définitions des données à caractère personnel[154], des traitements de ces données[155], ainsi que des fichiers[156] comportant les données sont posées d'un côté, quand les acteurs du monde numérique, notamment les responsables de traitement de données[157] ou le destinataire dudit traitement[158] sont désignés en parallèle. Ces innovations en matière de ligne directrice, de politique de l'utilisation de l'informatique sont notamment nées du rapport Tricot, qualifiant de démission le fait de "*s'en remettre entièrement à l'informatique pour apprécier des situations humaines*[159]".

Cependant, tandis que cette logique avait permis de proscrire en 1978 le profilage automatique[160], les dernières initiatives prises en matière de renseignement tendent à redessiner les contours des politiques

---

[153] Article 2 de la loi "*Informatique et Liberté*", alinéa 1.

[154] Article 2, alinéa 2 de la loi "*Informatique et Liberté*" : "*Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres*."

[155] *ibidem*...alinéa 3 :"*Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction*."

[156] *ibidem*...alinéa 3 :"*Constitue un fichier de données à caractère personnel, tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés*".

[157]Article 3 de la loi "*Informatique et Liberté*" : "*Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalité et moyens".*

[158] *Ibidem*....alinéa 2 : "*Le destinataire d'un traitement de données à caractère personnel est toute personne habilité à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données."*

[159] Voir le rapport public du Conseil d'Etat de 2001 : "*les autorités administratives indépendantes*", Paris, La documentation Française.

[160] Profilage automatique : prise de décision impliquant une appréciation sur un comportement humain, sur le seul fondement d'un algorithme établissant le profil de l'individu (Rapport du Conseil d'Etat, "*numérique et droits fondamentaux*", 2014, Paris, la documentation Française)

contemporaines liées à l'usage de l'Internet[161] : la sécurité policière menace alors de prendre progressivement le pas sur la « *sécurité humaine* ».

Section II/ Le droit d'accès à internet

L'accès à Internet revêt déjà de fondamental, la possibilité qu'il offre de garantir l'exercice de libertés fondamentales classiques comme la liberté d'entreprendre[162], la liberté d'association[163], ou de promouvoir un ensemble de droits fondamentaux[164] : en ce sens, il implique non seulement la liberté d'accéder à Internet (*Sous-section I*), mais encore le principe contemporain de" *neutralité de l'Internet"* (*Sous-section II*).

§.1/ La liberté d'accéder à Internet :

Le Conseil constitutionnel s'est prononcé sur le caractère fondamental de ce droit dans le cadre d'un recours formé contre la loi favorisant la diffusion et la protection de la création sur Internet qui confiait à la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet (HADOPI) :

Cette autorité disposait du pouvoir de prononcer une sanction administrative de suspension de l'accès Internet à l'encontre d'une personne qui, ayant fait l'objet de deux avertissements préalables, omettait de veiller à ce que l'accès Internet ne soit pas utilisé pour diffuser, recevoir des contenus en méconnaissance des droits d'auteur. Le Conseil constitutionnel releva en l'espèce que cette sanction de suspension de l'accès Internet pouvait "*conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile*", tandis que seule "(*...)l'autorité judiciaire est gardienne de la liberté individuelle*"[165] et que "*nul ne peut être puni qu'en vertu d'une Loi établie et promulguée antérieurement au délit, et légalement appliquée*"[166]. La condition formelle de légalité de la loi pénale, impliquant que la loi soit prise par le Parlement pour être considérée comme légalement appliquée,

---

[161] Voir *infra*... Partie II, Titre II, Chapitre II.

[162] Décision de conformité du Conseil constitutionnel n°81-132 du 16 janvier 1982 :"*Liberté qui, aux termes de l'article 4 de la Déclaration, consiste à pouvoir faire tout ce qui ne nuit pas à autrui, ne saurait elle-même être préservée si des restrictions arbitraires ou abusives étaient apportées à la liberté d'entreprendre*."

[163] Décision de conformité n°71-44 du 16 juillet 1971 : "*Considérant qu'au nombre des principes fondamentaux reconnus par les lois de la République et solennellement réaffirmés par le préambule de la Constitution il y a lieu de ranger le principe de liberté d'association*."

[164] "*L'accès à Internet est aussi bien un droit fondamental en lui-même qu'un "facilitateur" d'autres droits, comportant les droits économiques, sociaux et culturels, tels que le droit à l'éduction, le droit de prendre part à la vie culturelle et de jouir du progrès scientifique et de ses applications, ainsi que les droits civiles et politiques, tels que le droit d'association ou de réunion*", "*Report of the spécial Rapporteur on the promotion and protection of the right to freedom of opinion and expression*" LARUE Franck, Nations-Unies, mai 2011.

[165] Article 66 de la Constitution de 1958.

[166] Article 8 de la Déclaration des Droits de l'Homme et du Citoyen de 1789.

n'étant pas remplie en l'espèce, le Conseil constitutionnel déclarait inconstitutionnelle la mesure de suspension de l'accès Internet prise par HADOPI.

Plus précisément, dans cette décision du 10 juin 2009, le Conseil constitutionnel proclamait le caractère fondamental du droit d'accès à Internet en proclamant "*qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et opinions, [la liberté de communication protégée par l'article 11 de la Déclaration des Droits de l'Homme et du Citoyen] implique la liberté d'accéder à ces services*"[167].

Internet constitue donc un vecteur essentiel d'exercice de la liberté d'expression, et priver les citoyens de la possibilité d'accéder à ce service, restreignait mécaniquement la plénitude de l'exercice de cette liberté fondamentale : c'est à ce titre que l'accès à l'Internet constitue un droit fondamental, qu'il met à la charge de l'Etat l'obligation de ne pas couper l'accès au réseau.

§.2/ Le principe de neutralité d'Internet :

Le concept de "*neutralité du net*" est dégagé pour la première fois par le juriste américain Tim Wu[168] :

Il s'agit de garantir que "*le réseau public, pour qu'il puisse aspirer à être d'utilité maximale, traite tous les contenus, sites et plateformes de la même manière, ce qui lui permettrait de transporter toute forme d'information et d'accepter toutes les applications*." Dans une logique d'optimisation du réseau, l'ensemble des informations doit pouvoir jouir de la garantie du meilleur effort fourni par l'opérateur, sans garantie de résultat ni de discrimination, dans sa transmission d'un point à un autre. Il s'agit en fait de promouvoir la même liberté de circulation à toutes les informations, ce qui garantit non seulement l'optimisation du réseau Internet, mais encore la plénitude de l'exercice de la liberté d'expression.

Ce principe de "*neutralité de l'Internet"*, progressivement reconnu en France, s'inscrit dans un processus de normalisation de recommandations, d'évolution du droit mou jusqu'au droit dur :

Au premier stade, l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) formule en 2010 dix recommandations, lesquelles visent à respecter la liberté d'envoyer et de recevoir le contenu, à utiliser les services ou faire fonctionner les applications, connecter le matériel et utiliser les

[167] Décision de conformité du Conseil constitutionnel n°2009-580, §.12
[168] WU Tim, "*Network Neutrality, Broadland Discrimination*", Journal of Telecommunications and High Technology Law, Vol.2, p.141, 2003.

programmes de son choix, dès lors qu'ils ne nuisent pas au réseau[169] ou visent encore à respecter des critères de pertinence, proportionnalité, d'efficacité de non-discrimination dans les pratiques de gestion de trafic des opérateurs[170].

La normalisation de ces recommandations pourrait découler de la transposition de l'ensemble des réformes proposée au Parlement européen, connu sous le nom de "*troisième paquet télécom*" tandis que l'ordonnance du 24 août 2011, prise sur le fondement des directives européennes en matière de réseaux et services de communications électronique[171], ajoute à la liste fixée par l'article 32-1 du Code des postes et des communications électroniques, l'objectif de "v*eille à l'absence de discrimination, dans des circonstances analogues, dans les relations entre opérateurs et fournisseurs de services de communications au public en ligne pour l'acheminement du trafic et l'accès à ces services*".

Enfin, une proposition de règlement établissant des mesures relatives au marché unique européen des communications électroniques visant à faire de l'Europe un continent connecté[172] reprenait les recommandations formulées par l'ARCEP en matière de "*neutralité de l'Interne*t".

Cependant, reprenant la logique de la loi LOPPSI II visant à bloquer des sites à caractère pédopornographique, la loi du 13 novembre 2014 relative à la lutte contre le terrorisme prévoit dorénavant la possibilité pour l'autorité administrative de faire retirer les contenus de sites Internet provoquant directement à des actes de terrorisme ou faisant publiquement l'apologie de ces actes : le principe de « *neutralité de l'Internet »* est donc fortement tempéré, voire exclu par des impératifs sécuritaires qui, s'ils sont conjoncturels, engendrent des conséquences structurelles dans le cyberespace[173] : la nécessité de contrôler la normalité de l'activité numérique[174] prend alors nettement le pas sur l'objectif de protection des libertés personnelles.

Section III/ Le droit à l'oubli

Les dispositions de la directive européenne 95/46/CE impliquent que les internautes puissent demander, sous certaines conditions, la suppression des liens vers des informations portant atteinte à la vie privée (*Sous-*

[169] Recommandation n°1
[170] Recommandation n°3
[171] Directive 2009/136/CE "*service universel et droits des utilisateurs au regard des réseaux et services de communication électronique*"
Directive n°2002/58/CE "*traitement des données à caractère personnel et protection de la vie privée dans le secteur des communications électroniques*"
[172] Proposition 2013/0309 de règlement établissant des mesures relatives au marché unique européen des communications électroniques.
[173] Voir *infra* ...Partie II, Titre I, Chapitre II.
[174] On peut encore parler de "*biosécurité*"

section I) : la Cour de Justice de l'Union Européenne reconnaît d'ailleurs le caractère fondamental de ce nouveau "*droit à l'oubli*" (*Sous-section II*).

§.1/ Les dispositions de la directive 95/46/CE :

Dès 1995, les Etats membres de l'Union Européenne prenaient une directive visant à protéger les libertés et droits fondamentaux des personnes physiques, notamment ceux ayant trait à leur privée au regard des traitements de données à caractère personnel[175]. Cependant, ces droits personnels devaient être conciliés avec l'objectif de la libre circulation des données à caractère personnel entre Etats membres[176], de « *meilleur effort* » possible dans la circulation des données.

La directive précise surtout des notions importantes : la donnée à caractère personnel constitue ainsi « *toute information concernant une personne physique identifiée ou identifiable* »[177], quand le fichier de données à caractère personnel comprend « (..) *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminées* » : ce dernier peut alors faire l'objet de toute opération ou ensemble d'opération à l'aide de procédés automatisés, telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, ou encore le rapprochement ou l'interconnexion[178].

Le responsable du traitement s'entend quant à lui comme une personne physique ou morale, une autorité publique, un service ou tout organisme qui seul, ou avec d'autres, détermine les finalités et moyens du traitement de données à caractère personnel : à cet égard, les finalités et moyens sont déterminés par le droit national ou communautaire. L'article 4 prévoit en effet qu'il incombe aux Etats membres d'appliquer les dispositions nationales au regard de la directive lorsque traitement est effectué dans le cadres des activités d'un établissement du responsable du système de traitement[179], ou lorsque le responsable du traitement n'est pas établi sur le territoire de l'Etat membre[180] ou sur le territoire de la Communauté[181]. Parmi les règles prévues par la directive, les Etats membres sont tenus de garantir ainsi à toute personne concerné le droit d'obtenir dudit responsable de traitement la rectification, l'effacement ou le verrouillage des données en raison du caractère incomplet ou inexact des données[182].

[175] *Infra* Chapitre premier, Article premier, objet de la directive, alinéa 1.
[176] I*bidem*...alinéa 2
[177] *Infra* Article 2, définitions, a)
[178] Définition du traitement de données à caractère personnel, voir. Chapitre 1, article 2, b) de la directive.
[179] *Infra* Chapitre premier, article 4, alinéa 1, a)
[180] *Ibidem*…b)
[181] *Ibidem*…c)
[182] Section V, article 12.

Il ressort de l'ensemble de ces dispositions que la personne physique identifiée ou identifiable grâce aux données faisant l'objet du traitement, peut demander à l'établissement du responsable de traitement agissant sur le territoire de la Communauté, le retrait de données le concernant. Cependant, ces dernières devront avoir un caractère inexact et, ou incomplet.

§.2/ L'arrêt du 13 mai 2014 de la Cour de Justice de l'Union Européenne :

La Cour était saisie par la juridiction espagnole dans le cadre d'un litige opposant "*Google*" à l'autorité de protection des données personnelles :

L'autorité avait ordonné à la multinationale californienne de désindexer des données relatives à deux articles de presse évoquant les dettes passées et réglées par le plaignant, dans le but que celles-ci disparaissent des résultats de recherche fait sur le nom du plaignant.

La Cour rappela dans cette affaire que les exploitants de moteurs de recherche sont des responsables au sens de la directive, et qu'une conception large de la notion d'établissement doit être privilégiée : l'entreprise "*Google*", disposant d'une filiale en Espagne assurant la promotion et la vente des espaces publicitaires sur le moteur de recherche, relevait ainsi de cette catégorie, et constituait un établissement.

Par ailleurs, il s'agissait de rappeler que la personne pouvait s'adresser directement à un moteur de recherche pour obtenir la suppression des liens vers des pages Internet contenant des informations portant atteinte à sa vie privée, sans que ce droit ne soit pourtant absolu : le droit fondamental à la protection de la vie privée, notamment des données personnelles, devait ainsi être concilié avec l'intérêt économique du moteur de recherche. Dans ce souci de conciliation, la nature de l'information, sa sensibilité pour la vie privée de l'intéressé et l'intérêt que représente cette information pour le public à la recevoir, au regard notamment du rôle joué dans la vie publique par cette personne, devaient être interprétés de manière casuistique[183].

Or, dans le cas d'espèce, la Cour énonce qu' « e*u égard à la sensibilité des informations contenues dans les annonces pour la vie privée de ladite personne et au fait que leur publication initiale avait été effectuée 16 ans auparavant, la personne concernée justifie d'un droit à ce que ces informations ne soient plus liées à son nom au moyen d'une telle liste. Dès lors, dans la mesure où il ne semble pas exister, en l'occurrence, de raisons particulières justifiant un intérêt prépondérant du public à avoir (…) accès à ces informations (…) il*

[183] Voir l'article « *décision de la Cour de Justice de l'Union Européenne : les moteurs de recherche doivent respecter le « droit à l'oubli »* du 16 mai 2014, www.cnil.fr/nuage/tag.droit-a-loubli/

appartient à la juridiction de renvoi de vérifier que la personne peut (…) exiger la suppression desdits liens de cette liste de résultats »[184].

Chapitre III :

La mutation des droits fondamentaux dans l'espace numérique :

Certains des droits fondamentaux traditionnels, transposés sur le terrain numérique, ont nécessairement connu une mutation importante : les évolutions ayant affecté la "*liberté d'expression*" (***Section I***) ou la "*liberté personnelle*" en témoignent (***Section II***).

Section I/ La liberté d'expression

L'avènement d'Internet correspond au besoin contemporain de disposer d'une information toujours plus universelle, toujours plus rapide : à cet égard, le développement du numérique modifie substantiellement les régimes traditionnels de liberté d'expression (*Sous-section I*), mais consacre parallèlement un régime commun applicable sur le terrain numérique (*Sous-section II*).

§.1/ Des régimes juridiques traditionnels affectés :

La liberté d'expression était traditionnellement régie par des régimes juridiques distincts, et particulièrement adapté à chacun de ces usages :

La presse, diffusée sous la forme de journaux imprimés, était régie par la loi du 29 juillet 1881 quand la communication téléphonique assurée par les opérateurs de télécommunications était régie par le code des postes et télécommunications. Quant à la communication audiovisuelle assurée par câble ou satellite, le régime juridique applicable était fixé par la loi du 30 septembre 1986[185].

Ces trois libertés d'expression étaient notamment soumises à différents contrôles : la première était dispensée de "*contrôle a priori*", la seconde soumise au contrôle du secret des correspondances, quand la troisième était soumise au régime d'autorisation.

Avec l'avènement d'Internet, c'est la convergence de ces trois modèles de libertés d'expression qui est privilégiée : aujourd'hui, le réseau permet, sinon incite à la diffusion de ces trois modes d'expression sur une

[184] Arrêt du 13 mai 2014, « *Google Spain* », Cour de Justice de l'Union Européenne, §.99
[185] *Op.Cit*…« *numérique et droits fondamentaux* »*Ibidem*…. p.100 et ss.

même plateforme. Face à ce phénomène de convergence, le législateur dût uniformiser les différents régimes jusqu'alors applicables.

La loi pour la confiance dans l'économie numérique du 21 juin 2004[186] a eu pour objet de transposer la directive « *commerce électronique* »[187], et catégorise désormais les modes d'exercice de la liberté d'expression : on parle ainsi des « *communications électroniques* », lesquelles regroupent les « *communications au public par voie électronique* » et les communications ayant le caractère d'une correspondance privée[188]. Les « *communications au public par voie électronique* » comprennent notamment la « *communication au public en ligne* »[189], et la communication audiovisuelle[190] .

Pour ce qui est des acteurs, la loi de transposition fixe encore deux grandes catégories : il s'agit des éditeurs de services sur Internet et des hébergeurs. Les premiers ne sont soumis à aucune obligation de déclaration préalable, ou d'autorisation, quand les limites à leur liberté d'expression sont fixées par la loi du 28 juillet 1881[191], et que leur droit de réponse est prévu par la loi sur la confiance dans l'économie numérique de 2004. Concernant les seconds[192], ils sont quant à eux responsables pénalement et civilement au même titre que les opérateurs téléphoniques, s'ils avaient connaissance de l'activité illicite ou, si après avoir été informés, ils n'ont pas agi promptement pour retirer le contenu ou le rendre inaccessible.

Enfin, une nouvelle catégorie juridique intermédiaire de « *services de médias audiovisuels à la demande* » est apparue : elle regroupe les services de télévision de rattrapage et de vidéo à la demande, et soumet ces services à des obligations de diffusion d'œuvre européennes, de soutien à la production, de protection des mineurs[193].

§.2/ Un régime commun encadré :

La démocratisation de l'outil Internet appelle à des initiatives en matière de protection des droits qui trouvent à s'exercer sur le terrain numérique, quand la jouissance de ces droits reste cantonnée à la sphère d'exercice des droits et libertés fondamentaux d'autrui :

---

[186] Loi n°2004-575 du 21 juin 2004 pour la « *confiance dans l'économie numérique* ».
[187] Directive n°2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.
[188] Les correspondances privées comprennent les courriels et le téléphone.
[189] La communication au public en ligne correspond au « web » et assure un échange réciproque d'informations entre l'émetteur et le récepteur.
[190] La communication audiovisuelle comprend les services de radio et télévision.
[191] Loi du 29 juillet 1881 relative à la liberté de la presse, chapitre IV.
[192] L'article 6, alinéa 1, 2) les définit comme des « *personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute autre nature fournis par des destinataires de ces services.* »
[193] Directive n°2010/13/UE du Parlement européen et du Conseil du 10 mars 2010, « *directive services de médias audiovisuels* ».

La liberté d'expression est ainsi tempérée par les nécessités de lutte contre les actes de provocation à la discrimination ou à la haine envers des personnes en raison de leur origine, de leur religion ou de leur orientation sexuelle, contre les actes de négation de crimes contre l'humanité, de diffamation, d'injure ou encore de révélation de l'identité d'agents des services de renseignement. Dans cette logique, les pouvoirs publics ont notamment pris certaines mesures propres à assurer la régulation de l'usage d'Internet :

la loi LOPPSI II ajoute ainsi à l'article 6 de la loi du 21 juin 2004 pour la Confiance dans l'Economie Numérique (LCEN) les dispositions suivant lesquelles, "*lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal*[194] *le justifient, l'autorité administrative notifie (...) les adresses électroniques des services de communication a public en ligne contrevenant aux dispositions de cet article auxquelles (...) doivent être empêcher l'accès sans délai*".

Parallèlement, la LCEN prévoit l'obligation pour les fournisseurs d'accès à internet et les hébergeurs de mettre en place un dispositif de signalement des contenus illicites, sinon de retrait des contenus signalés, les service intéressés[195] sont appelés à définir des mesures de police sur les contenus autorisés allant de l'interdiction des appels à la violence, la lutte contre la xénophobie, ou l'objectif de lutte pour la protection des mineurs. Cependant, afin de concilier le objectifs de sécurité en matière d'économie numérique avec le "*principe de neutralité de l'Internet*", et de circulation libre de l'information, les fournisseurs ne sont pas soumis à une obligation générale de surveillance, ou d'enquête sur les faits ou circonstances révélant ces activités illicites[196]

Enfin, faisant écho à la loi LOPPSI II, mais justifiée cette fois par des nécessités de lutte contre la provocation à des actes terroristes, l'article 12 de la loi du 13 novembre 2014 prévoit désormais la possibilité de retirer les contenus des sites provocant ou faisant l'apologie du terrorisme : néanmoins, l'autorité administrative ne dispose plus de la seule faculté de notifier les adresses électroniques de ces services de communication, mais peut désormais de sa propre initiative, en l'absence de retrait de ces contenus dans un délai de vingt-quatre heures, procéder d'office au retrait de ces contenus.

---

[194] Article 227-23 du code pénal : "*Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils ont pas été commis en vue de la diffusion de cette image ou représentation.*"

[195] Les services comme « *Facebook* », « *Twitter* », « *Youtube* » ou « *Dailymotion* » par exemple

[196] Article 6, alinéa 7 de la LCEN : "*les personnes (fournisseurs d'accès Internet et hébergeurs) ne sont pas soumis à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites (...) sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire.*"

Section II/ La liberté personnelle

La liberté personnelle recouvre traditionnellement le droit à la vie privée, l'inviolabilité du domicile, la liberté d'aller et de venir... Si certains de ces droits et libertés fondamentaux sont aujourd'hui menacés sur le terrain numérique (*Sous-section I*), de nouveaux moyens numériques à disposition des autorités de poursuite ont nécessairement été développés (*Sous-section II*).

§.1/ L'émergence de nouvelles menaces liées au numérique

La Convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité[197] dresse un panorama des différentes menaces numériques pour les droits fondamentaux des internautes :

Cet instrument distingue les menaces numériques selon qu'elles entrent dans la catégorie des "*infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes d'informations*", dans celle des "*infractions numériques*", des "*infractions se rapportant au contenu*" ou dans les "*infractions liées aux atteintes la propriété intellectuelle et aux droits connexes*". Plus schématiquement, le Conseil d'Etat distingue dans son étude annuelle relative au "*numérique et [aux] droits fondamentaux*", les atteintes à la sécurité qui ont pour cible le numérique en visant à entraîner le dysfonctionnement d'un système informatique, et celles pour lesquelles le numérique est un moyen de commettre une infraction. Enfin, certaines infractions entrant dans le champ d'application des atteintes ayant pour cibles des atteintes à la sécurité sont spécifiques, car relevant d'atteintes spécifiques contre les intérêts fondamentaux de la Nation[198].

Cependant, on peut aujourd'hui dresser une autre typologie des menaces sur le terrain numérique : la première catégorie regrouperait l'ensemble des infractions commises sur le cyberespace, selon que le numérique constitue le moyen de commettre l'infraction ou la cible principale de l'infraction. La seconde catégorie regrouperait quant à elle les atteintes à caractère informationnel, selon qu'elles visent à diffuser ou propager des informations d'une part, qu'elles soient à fin publicitaire, personnelle, ou même terroriste ou selon qu'elles visent à recueillir des informations confidentielles cette fois. Là encore il s'agira autant d'informations personnelles, que commerciales, politiques ou même militaires.

Cette dernière typologie nous permettra notamment de confronter deux modèles de sécurité contemporaine par la suite : le premier relèverait du modèle policier hybride, à mi-chemin entre police politique privilégiant le renseignement intérieur, et sécurité militaire mettant l'accent sur les intérêts d'Etats dans un contexte de balance des puissances sur le terrain géopolitique (*Voir le tableau en annexe II pour une présentation schématique des différentes modèles contemporains de sécurité*), quand le second aurait trait cette fois au

[197] "*Convention de Budapest*"
[198] *Op.Cit…* "le *numérique et droits fondamentaux*" *Ibidem…..* pp.144 et ss.

modèle de "*sécurité humaine"* qui privilégierait la protection des populations face à la défense des intérêts d'Etats, tendant progressivement à mettre l'Etat au service des individus, et non plus à contraindre les individus à être au service des Etats.

Or, si on compte autour de 35millions de victimes directes du fait des guerres interétatiques, pour 165 à 170millions de victimes massacrées par leurs propres Etats au XXème siècle[199], le phénomène conduirait à repenser la notion de souveraineté traditionnelle. Il s'agirait aujourd'hui de privilégier la souveraineté des individus sur la souveraineté des Etats[200], d'entendre non plus la souveraineté comme un droit classiquement absolu (droit de guerre, calcul froid des intérêts) mais comme un devoir, une "*responsabilité de protéger*" les populations à la charge de l'Etat.

§.2/ Le développement de nouveaux dispositifs à disposition des autorités de poursuite.

Le "*Big Data*" a conduit à renforcer l'efficacité des moyens d'action de la police, que celle-ci ait pour tâche de "*constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs*"[201], ou qu'elle ait pour tâche de sauvegarder l'ordre public en prévenant les infractions. Le renseignement fera l'objet d'une plus approfondie par la suite[202].

Le numérique, quand il ne conduit pas à optimiser l'usage de modes traditionnels d'investigation, permet de développer de nouveaux modes opératoires inédits[203]. Il ne sera cependant question que des modes d'investigation traditionnels ici[204] :

Le numérique conduit notamment à optimiser l'usage des fichiers de police en permettant l'interconnexion des différentes informations utilisées et, ou conservées : le "*Traitement d'Antécédents Judiciaires*" (TAJ) a notamment permis de faire fusionner le "*Système de Traitement des Infractions Constatées*" (STIC) de la police nationale avec le "*Système Judicaire de Documentation et d'Exploitation*" (JUDEX) de la gendarmerie nationale, il regroupe aujourd'hui 12,2 millions de fiches sur des mis en cause et permet dorénavant de procéder à des enquêtes administratives concernant le recrutement à des emplois présentant une sensibilité particulière depuis la loi du 18 mars 2003 sur la sécurité intérieure. Parallèlement, le Fichier des Personnes Recherchées (FPR) rassemble les informations relatives à l'ensemble des personnes recherchées ou disparues, dans le cadre de la police judiciaire ou de législations administratives spécifiques

[199] *Op.Cit*…"*Le Principe Sécurité*" *Ibidem*…. p.187 et ss.
[200] ANNAN Kofi, "*Deux concepts de la souveraineté*", "*Le Monde*", 22 septembre 1999.
[201] Article 14 du Code de procédure pénale.
[202] Voir *infra* ...Partie II pour ces développements.

[203] *Op.Cit*… " le *numérique et droits fondamentaux*" *Ibidem*….117 et ss.
[204] Les nouveaux modes d'investigation seront vus dans la Partie II

(législation applicable sur le droit des étrangers par exemple) : il regroupait quelques 400 000 fiches au 1er novembre 2010 selon les estimations de la CNIL.

La conservation et l'utilisation des données biométriques[205] à des fins de comparaison a aussi été optimisée par l'utilisation des technologies liées au numériques : si le nombre d'intéressés par le Fichier National Automatisé des Empreintes Digitales (FNAED) regroupait environ 900 000 personnes en 1997, il avoisine en 2008 les 3millions de personnes quand le Fichier National Automatisé des Empreintes Génétiques (FNEG), s'il regroupait un ensemble de 2 635 personnes en 2002, concerne 806 356 personnes en 2008 avant d'atteindre à son tour les 2 millions de personnes en 2012.

Enfin, le procédé de classique de vidéosurveillance est aussi affecté, à tel point que l'on parle dorénavant de "*vidéo-protection intelligente*"[206] : c'est que le nombre de ces "*learning machines*", capables de détecter des mouvements atypiques, de reconnaître un visage, ou de lire automatique des plaques d'immatriculation concernait déjà un ensemble de 70 000 caméras sur la voie publique en 2011. Un an plus tard, elles sont au nombre de 935 000 sur l'ensemble du territoire, tandis que la CNIL n'a opéré que 150 contrôles de cette activité, pour une vingtaine de sanctions prononcée[207].

Aujourd'hui, si le numérique constitue un vecteur de protection de certains droits fondamentaux classiques, en plus de constituer un foyer d'émergence de nouveaux droits fondamentaux (**Partie I**), il reste cependant un formidable outil de surveillance, sinon de contrôle des comportements individuels dans la société justifié par les risques de menaces, notamment terroristes sur le terrain numérique (**Partie II**).

[205] Invention d'Alphonse Bertillon datant de la fin du XIXème siècle, visant à recueillir les empreintes digitales.
[206] Ministère de l'intérieur, de l'outre-mer et des collectivités locales, "*note technique : la vidéo-protection intelligente*", juillet 2008.
[207] POLLONI Camille, "*Les cinq chiffres (fous) de la vidéosurveillance*", "*les inrocks*", 21 juin 2012

PARTIE II /

Le développement de nouvelles menaces pour les droits fondamentaux, nécessité de contrôle des usages lié au numérique pour nos sociétés contemporaines?

Biosécurité : "*Ensemble des mesures destinées à assurer la continuité d'un processus*."
(« *Le Principe Sécurité* », Frédéric Gros, 2012.)

Le processus de numérisation de la société appelle mécaniquement à concevoir de nouveaux dispositifs de sécurité adaptés (**Titre I**) : il s'agit de fournir des réponses réelles face à des menaces virtuelles (**Titre II**), d'assurer un nouveau type de sécurité au sein d'interactions pourtant classiques (**Titre III**).

Titre I / Numérisation des moyens sécuritaires :

La démocratisation de l'utilisation du réseau Internet suscite non seulement l'émergence de nouveaux acteurs de sécurité (**Chapitre I**), mais aussi le développement de nouvelles menaces contemporaines : les « *atteintes informationnelles* » (**Chapitre II**).

Chapitre I :

Nouveaux acteurs

Aujourd'hui, Il s'agit moins de promouvoir la sécurité de l'entreprise face aux nouvelles menaces numériques, que d'assurer la sécurité des Etats face aux multinationales en situation d'oligopole sur le marché de l'Internet (***section I***), tandis que l'implication de ces nouvelles technologies dans la vie des citoyens conduit à promouvoir l'utilisation de nouveaux dispositifs de sécurité, comme la cryptographie. (***Section II***).

Section I / Multinationales

Les logiques concurrentielles entre Etats conduisent à ériger les multinationales en menaces potentielles pour la souveraineté des Etats sur la scène internationale (*Sous-section 1*), quand la concurrence privée implique le développement des risques corrélés à l'usage de nouvelles technologies pour les entreprises privées, comme publiques : l'émergence des technologies du numérique justifie le développement de nouvelles stratégies de sécurité, la création de nouvelles structures de type militaire (*Sous-section II*).

§.1/ Menaces ou acteurs de la sécurité ?

Selon le journaliste Dan Schiller, certaines des multinationales appartenant au groupe GAFA[208] « *(...) auraient bâti leur fortune sur l'espionnage à grande échelle dans un but commercial* »[209] :

A cet égard, les modifications de l'architecture initiale d'Internet, privilégiant le passage à l'informatique en nuage sur les outils personnels de conservation des données personnelles, s'inscrivent notamment dans des « *(...) stratégies de profit des entreprises reposant explicitement sur les données de leurs utilisateurs* »[210], sur la vente des données personnelles enregistrées par les « *objets interconnectés* » aux annonceurs et autres sociétés. Ces pratiques conduisent alors les Etats à se prémunir des risques engendrés par la surveillance, sinon la vente des données personnelles de leur population, à développer de nouvelles solutions de sécurité :

Certains Etats jugent en effet nécessaire de réorienter leur politique économique relative au numérique vers des solutions réservant la possibilité de conserver les données des citoyens aux seuls fournisseurs nationaux : c'est par exemple le choix privilégié par la Russie aujourd'hui. C'est qu'actuellement, les pratiques des multinationales en situation d'oligopole sur le marché numérique sont déterminantes dans les choix stratégiques en matière de sécurité militaire : l'Allemagne a par exemple mis un terme au contrant qui l'unissait de longue date à la compagnie américaine « *Verizon* » au profit de « *Deutsche Telekom* », tandis que le Brésil et l'Union européenne prévoient de construire de nouveaux réseau de télécommunications sous-marins pour que leurs communications intercontinentales n'aient plus à dépendre des infrastructures américaines. Enfin, au niveau local cette fois, la ville de Brasilia a choisi d'abandonner le service de messagerie « *Outlook* » au profit d'un système utilisant des centres de donnée implantés sur son territoire, tandis que certaines voix ont pu s'élever sur le territoire national en 2009 vers des propositions de nationalisation du réseau Internet[211], option d'ailleurs privilégiée de longue date par la Chine.

Les multinationales constituent donc actuellement plus des menaces pour la sécurité des Etats, concernant notamment la défense de leurs intérêts nécessaire à l'équilibre de la balance des puissances, que des acteurs de la sécurité à proprement parler, sauf lorsqu'elle sert des intérêts étatsuniens.

§.2/ la sécurité des entreprises, quelles menaces pour quelles réponses ?

Le développement des technologies du numérique a entraîné une multiplication des risques et menaces pesant sur les entreprises :

---

[208] L'acronyme « *GAFA* » recouvre les quatre principales multinationales en situation d'oligopole sur le marché de l'Internet, à savoir : « *Google* », « *Amazon* », « *Facebook* », « *Apple* ».
[209] SCHILLER Dan, « *Géopolitique de l'espionnage* », in « *Le Monde Diplomatique* », Novembre 2014.
[210] MOROZOV Evgeny, « *De l'utopie numérique au choc social* », in « *Le Monde Diplomatique* », Août 2014.
[211] « *Un député UMP propose de nationaliser le réseau Internet* », Article, tempsréel.nouvelobs.com, 17 décembre 2009.

A cet égard, une enquête menée par l'EDHEC et le CDSE portant sur les crimes commis contre les entreprises en 2008 et 2009[212] illustrait les menaces pesant sur l'ensemble des constituantes de l'entreprise : « *[elles concernent ainsi…] ses ressources techniques, humaines et financières, son organisation, ses champs d'opération, sa compétitivité et même sa propriété (…) : ses ressources sont volées, détournées, dégradées, voire détruites ; son organisation est utilisée pour le développement de trafics illicites ou pour les blanchiment d'argent sale ; sa concurrence est constituée de groupes criminels quand sa compétitivité se trouve affaiblie par la contrefaçon ou l'espionnage ; enfin, la propriété fait l'objet de convoitises et fait l'objet de tentatives d'entrée dans son capital par des acteurs criminels…* [213]».

L'enquête révèle que le crime est un phénomène qui fait aujourd'hui partie de la vie des entreprises : « *ce ne serait plus une menace, mais un fait avéré*[214] ». Si les acteurs aux agissements criminels sont principalement les propres employés de l'entreprise (87%), quand les crimes les plus courants sont l'espionnage et, ou les vols sur site, les entreprises doivent se rapprocher le plus souvent de nouveaux acteurs : il s'agit pour elles, sans considération de leur taille ou de leur degré d'internationalisation, de s'entourer dorénavant d'entreprises de sécurité/sûreté ou de forces de police dans la majorité des cas (96% et 93%). Les consultants en intelligence économique ou en sécurité sont aussi largement sollicités (87%), comme les compagnies d'assurance (80%) ou les associations de directeurs de la sécurité/sûreté (79%.).

Si cette augmentation des menaces numériques pesant sur les données des entreprises a notamment été corroborée la même année par une étude menée par le réseau d'entreprises américaine spécialisée dans l'audit, l'expertise comptable et le conseil « *PricewaterhouseCoopers* », les pouvoirs publics ont été contraints de créer une nouvelle structure chargée de lutter contre la prolifération des menaces numériques pesant sur le patrimoine économique Français : l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Ce service à compétence nationale, rattaché au Secrétaire Général de la Défense et de la Sécurité Nationale (SGDSN), créé par décret du 7 juillet 2009, sera dorénavant chargé (…)*d'assurer la mission d'autorité nationale en matière de sécurité des systèmes d'informations (…) de proposer des règles à appliquer pour la protection des systèmes d'information de l'Etat et de vérifier l'application des mesures adoptées (…)*[215] », son objectif de conserver l'intégrité du patrimoine économique Français largement en situation de dépendance au numérique aujourd'hui.

---

[212] «*Enquête EDHEC-CDSE : Panorama 2008 et 2009 des crimes commis contre les entreprises », « Dossier /2010-2020 une nouvelle décennie de menaces ?* » VERY Philippe, MONNET Bertrand, HASSID Olivier, revue « *Sécurité et Stratégie* » n°3, mars 2010, p.6 et ss.

[213] *Op.Cit… « Panorama 2008 et 2009 des crimes commis contre les entreprises » … Ibidem* p.9 et ss.

[214] *Op.Cit… « Panorama 2008 et 2009 des crimes commis contre les entreprises» Ibidem….* p.10

[215] Présentation des missions sur le site de l'ANSSI :
www.ssi.gouv.fr

Section II / Particuliers

La cryptographie, objet classiquement mis à la disposition des autorités au service du principe de sécurité militaire (*Sous-section I*), constitue aujourd'hui un outil alternatif, mais avantageux aux mains des particuliers en matière de sécurité numérique : elle fait désormais de ces derniers, les acteurs à part entière de leur sécurité juridique (*Sous-section II*)

§.1/ L'outil traditionnel de sécurité des correspondances, la cryptographie :

La « *cryptologie*[216] », dont l'application pratique est la cryptographie, apparaît à ce jour comme l'unique moyen de sécuriser les correspondances échangées sur Internet par, et pour les particuliers[217] :

La loi du 26 juillet 1996 relative à la réglementation des communications dispose que la cryptographie vise à " *transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers* ", son objet consiste donc à cacher les informations d'un message dans le but d'assurer la confidentialité, garantir l'authenticité et conserver l'intégrité des informations échangées. En recourant au procédé, les utilisateurs peuvent ainsi se prémunir des menaces pesant sur leurs communications.

Concernant la confidentialité, elle vise à garantir lors de toute expédition ou réception d'un message que les informations soient utilisables uniquement par son destinataire légitime, et à empêcher qu'un tiers n'ait la possibilité d'exploiter les informations transmises, même si celles-ci devaient tomber en sa possession.

L'authenticité apparaît quant à elle comme un moyen de prévenir l'action d'un correspondant malveillant par le biais de l'identification du producteur de l'information au moyen d'une signature comme gage d'authenticité : elle permet notamment de s'assurer que l'émetteur ne puisse pas nier les avoir envoyées, et aura pour corollaire le principe de non-répudiation qui permet de garantir à l'expéditeur la réception effective de son message par le correspondant.

Conserver l'intégrité des informations permet enfin de s'assurer que ces dernières, une fois reçues, sont bien celles émises par l'émetteur : elle vise à empêcher que leur modification ou altération par un tiers soit indécelable ou possible.

---

[216] Le terme est issu des termes grecs « *kryptos* » et « *logos* » qui signifient respectivement « *caché* » et « *langage* » : la cryptologie signifie ainsi la science du langage.

[217] BOISSEAU Gaël, "*Tiers de confiance ou de défiance ?* », La sécurité collective face à la cryptographie asymétrique, Cahiers de la Sécurité Intérieure, n°34, 4° trimestre 1998, Institut National des Hautes Etudes sur la Sécurité et la Justice, p.31-35.

§.2/ La cryptographie appliquée à la sphère numérique : outil de sécurité adapté au bénéfice des particuliers.

Cependant, dans le cyberespace, réseau informatique en tant que tel ou l'information qui y circule est destinée à être traitée par des ordinateurs, toute personne accédant à l'information peut la dupliquer, la modifier et surtout l'utiliser[218] :

A ce titre, Internet ne présente aucune garantie au regard des trois finalités visées par la cryptographie traditionnelle (« *assurer la confidentialité* », « *garantir l'authenticité* », « *conserver l'intégrité* »). Pour remédier à ces lacunes, la cryptographie moderne va transformer les données en insérant une fonction supplémentaire : l' « *algorithme* ».

Ce nouvel outil va dorénavant permettre à l'utilisateur de crypter ses données en utilisant l'algorithme standard et une clef logique qui permettra d'assurer une permanence de la sécurité dans l'hypothèse où l'algorithme est connu[219] : le recours à la clef logique, en plus de l'algorithme, fera donc en principe obstacle à ce qu'une personne comprenne le mécanisme de chiffrement utilisé.

Cependant, si l'usage en réseau de la cryptographie implique que le destinataire d'un message dispose de la clef ayant servi à le crypter, le seul moyen offert à l'émetteur consiste à transférer au destinataire cet objet, ce qui constitue une première faille dans le système de sécurité. Dans cette logique, les auteurs Whitfield Diffie et Martin Hellman ont donc inventé dans les années soixante-dix la cryptographie asymétrique : ce nouveau procédé consistait à utiliser un couple de clefs dont une seule était diffusée, ce qui supprimait le problème de la sécurité de leur transmission, et permettait d'assurer la confidentialité des messages et leur intégrité.

En définitive, les particuliers deviennent progressivement les propres acteurs de leur sécurité, et disposent de certains dispositifs nécessaires et adaptés pour assurer la protection de leurs données et informations personnelles aujourd'hui, comme témoigne la cryptographie asymétrique : le numérique conduit alors au développement de nouveaux dispositifs de sécurité collective, sinon juridique aux mains du collectif citoyen.

Chapitre II :

Nouvelles menaces pour la sécurité dans l'espace numérique, les atteintes informationnelles

Les atteintes informationnelles visent deux finalités, mais concernent un même objet : les informations sensibles. Elles consisteront donc soit à propager ou diffuser des informations sensibles visant à troubler l'ordre public au sein même du territoire (***Section I***), soit à recueillir ou soustraire des informations

[218] Op.Cit… « *Tiers de confiance ou de défiance ?* »
[219] Kerchkoffs, 1883

sensibles, dans le but cette fois d'impacter la sphère d'influence de l'Etat sur la scène internationale (***Section II***).

Section I : Atteintes visant à diffuser, propager des informations sensibles.

Les atteintes numériques visant à diffuser, propager des informations sensibles sont aujourd'hui plus que jamais d'actualité, comme en témoigne l'exemple du « *cyber terrorisme* » (*Sous-section I*). Elles représentent non seulement une menace pour le principe de sécurité policière, à l'intérieur du territoire national, mais encore pour le principe de sécurité militaire, quand elles transcendent les frontières (*Sous-section II*).

§.1/ Les atteintes visant à diffuser des informations sensibles : l'actualité du « cyber terrorisme ».

La banalisation de l'outil numérique, et l'augmentation exponentielle de son nombre d'utilisateurs a favorisé l'émergence d'infractions pénales dans l'environnement numérique : celles-ci concernent aujourd'hui principalement les faits d'association en relation avec une entreprise terroriste[220] .

C'est qu'Internet est devenu non seulement un moyen de diffusion d'une idéologie terroriste, mais aussi un moyen de recruter de nouveaux combattants pour ces organisations : si hier encore, l'organisation terroriste « *Al Qaeda*[221]» se servait d'Internet pour diffuser des scènes d'exécution, comme celle filmée en mai 2004 et reprise par tous les médias par la suite[222], il est aujourd'hui principalement question de l'Organisation de l'Etat Islamique (OEI ou « *Daech »*) :

L'organisation se démarque sur la scène médiatique en utilisant des outils de propagande très perfectionnés et dispose notamment d'une aile média, dénommée « *Al-Hayat*[223]», qui a par exemple diffusé le film de propagande « *Flames of War* », traduit de l'arabe à l'anglais, dans lequel sont tournées des scènes de bataille en Syrie et en Irak, où sont promues les missions suicides, mises en avant les différentes origines géographiques des combattants, soulignant ainsi l'universalité du « *djihad* ».

Ce documentaire, dont on ne sait pas exactement s'il repose sur un ensemble de scènes réelles ou non, vise ainsi surtout à démontrer la capacité militaire de l'organisation[224] ; cependant le but subsidiaire de cette

---

[220] "*Cyberdroit : le droit à l'épreuve d'internet*", FERA-SCHUHL Christianne, Dalloz, 6° édition, 2011-2012, p.959 et ss.
[221] "*Al Qaeda*" signifie « la base » en arabe
[222] Le vendredi 18 juin 2004, l'otage Paul Johnson était décapité par l'organisation.
[223] "*Al Hayat*" signifie « la vie » en arabe
[224] Le documentaire, ou docu-fiction selon les avis, dure 55minutes. Il est filmé en très haute définition, et fait l'objet d'une introduction « *hollywoodienne* »

œuvre, par le biais notamment de la traduction de l'arabe vers l'anglais ou par la promotion des différentes ethnies s'alliant au « *djihad* », vise à recruter des combattants potentiels résidant pour une part en Europe[225].

En dehors de toute activité terroriste, les atteintes de diffusion, propagation des informations recouvrent par ailleurs les individus ou groupes éditant des recettes d'explosifs ou d'engins incendiaires : il s'agit notamment du « *Manuel du terroriste* » en libre accès sur le web, qui « (…) *décrit méthodiquement, de manière presque clinique, en dix-huit leçons comment se fondre dans le paysage d'un pays occidental, échapper aux poursuites, recruter, recueillir de l'information, fabriquer de faux papiers, détruire etc. (...)* ». Aussi étonnant que cela puisse paraître, on peut trouver le synopsis de ce libre « *fascinant* » sur le site amazon.fr[226]…

Ces menaces numériques ont nécessairement conduit le législateur à prendre de nouveaux moyens propres à prévenir ces atteintes informationnelles : désormais, on trouve dans le code pénal « *l'infraction de diffusion du mode d'emploi et de fabrication d'armes et de moyens de destruction*[227] », dont la peine est aggravée lorsque cette infraction est commise par un réseau de télécommunications à destination d'un public non déterminé[228] ou des infractions comme « *les menaces de destruction, réelles ou supposées*[229] *»* :

La loi du 13 novembre 2014[230] renforçant les dispositions relatives à la lutte contre le terrorisme est venue élargir le champ des infractions susceptibles d'être commises à des fins terroristes[231], en renvoyant aux dispositions contenues aux articles 322-6-1[232] et 322-13[233] du code pénal : les peines encourues pour ces infractions sont parallèlement aggravées, selon la gradation prévue à l'article 421-3 du même code.

Surtout, la loi est venue créer le « *délit d'apologie et de provocation au terrorisme* », lequel sanctionne dorénavant le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes[234] :

---

[225] www.tvqc.com/flames-of-war-letat-islamique-isis-publie-documentaire-propagande/

[226] http://www.amazon.fr/Al-Qaida-Manuel-pratique-du-terroriste/dp/2874950572

[227] Article 322-6-1 du Code pénal : "*est sanctionnée d'une peine d'un an d'emprisonnement et de 15 000euros d'amende, le fait de diffuser par tout moyen, sauf à destination des professionnels, des procédés permettant la fabrication d'engins de destruction élaborés à partir de tout autre produit destiné à l'usage domestique, industriel ou agricole*."

[228] Infraction punie d'une peine de trois ans d'emprisonnement, et de 45 000euros d'amende.

[229] Article 322-12 du Code pénal : "*est sanctionnée d'une peine de six moins d'emprisonnement et de 7 5000euros d'amende, le fait d'avoir menacé une personne physique de commettre une destruction et, ou détérioration »*

[230] Loi n°2014-1353 du 13 novembre 2014.

[231] La liste des infractions figure à l'article 421-13 du code pénal.

[232] *Infra* note de bas de page 183.

[233] *Infra* note de bas de page 185.

[234] L'article 421-2-5 du code pénal : « *le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000euros d'amende. Les peines sont portées à sept ans d'emprisonnement et à 100 000euros d'amende lorsque les fait ont été commis en utilisant un service de communication au public en ligne. Lorsque les faits sont commis par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne,*

Lorsqu'il s'agit d'apologie, la condition de publicité consistant à présenter ou commenter les actes de terrorisme en portant sur eux un élément moral favorable doit cependant être remplie, mais lorsqu'il est question de provocation, cette dernière condition n'est plus nécessaire à la consommation de l'infraction. La provocation devra cependant être une incitation directe, non seulement dans l'esprit mais également dans ses termes : elle doit persuader de commettre des faits matériellement déterminés.

Quand l'infraction est constituée sur le terrain numérique précisément, son auteur encourt la peine prévue pour le délit de provocation à la commission des infractions énumérées dans l'article 24 de la loi du 29 juillet 1881, pour laquelle joue le jeu des circonstances aggravantes : La peine de cinq ans d'emprisonnement et de 75 000euros d'amende initialement prévue, passe ainsi à sept ans et à 100 000euros d'amende lorsque la provocation est directe, ou lorsque l'apologie publique de ces actes est commise par le biais d'un service de communication au public en ligne.

§.2/ L'implication des atteintes visant à diffuser des informations sensibles sur le principe de sécurité policière politique :

Bien qu'aujourd'hui « *(...)90% des individus qui basculent dans le terrorisme le font par Internet* » selon le ministre de l'Intérieur[235], la menace terroriste reste quant à elle un phénomène ancien. Cependant, l'émergence des technologies lui permet non seulement d'être protéiforme, mais surtout persistante dans l'avenir[236] :

Comme le rappelle le professeur Yves Mayaud, l'originalité de la menace terroriste se situe dans sa finalité : il s'agit en effet « (…) *d'une criminalité très particulière, à base de conception, d'organisation et de réalisation d'infractions dont l'effet doit dépasser les victimes directes, telle une réaction en chaîne, pour atteindre la collectivité dans son ensemble* »[237]. Il s'agit donc moins d'atteindre l'intégrité des personnes physiques, que la cohésion de la collectivité ; d'ébranler une conception individuelle, plutôt qu'un modèle d'Etat.

La propagation d'informations sensibles présente donc un danger pour la sécurité de l'Etat avant tout, car elle permet de persuader, sinon d'endoctriner des individus résident ou non à l'intérieur du territoire dans une lutte ou s'affrontent deux conceptions idéologiques, ou politiques différentes :

---

les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

[235] Déclaration du ministre de l'intérieur, Mr. Bernard Cazeneuve du 4 février 2015.

[236] Projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

[237] MAYAUD Yves, « *Le terrorisme, connaissance du droit* », Dalloz, 1997.

Concernant l'Etat de droit par exemple, il s'agira de confronter la vision que s'en fait l'Occident, reposant sur la Constitution et un ensemble de règles de droit, avec la vision que s'en fait cette fois l'Organisation de l'Etat Islamique (OEI) ou le fondement principal sera la « *Charia* ». Or, dans un cas comme dans l'autre, il s'agira bien d'un Etat de droit sans que ce dernier ne repose sur les mêmes fondements, ou conceptions. A cet égard, la France constitue une cible prioritaire d' « *Al Qaeda* » depuis que la loi du 15 mars 2004 est notamment venue proscrire le port de signes religieux à l'école, ou depuis de son engagement au sein de la force internationale d'assistance et de sécurité en Afghanistan, sa position sur la question des relations libano-syriennes : il s'agit donc de critiquer, sinon de sanctionner la position défendue par l'Etat, sans considération particulière de celle adoptée par les individus[238].

Ces menaces sont notamment alimentées par la diffusion des technologies numériques qui, si elles touchent de plus en plus de personnes sur le globe et visent avant tout à faciliter la circulation d'informations, peuvent constituer des terrains propices à la critique des positions défendues par certains Etats. La propagande, si elle atteint aussi bien les personnes résident à l'intérieur du territoire national[239], que celles résidant à l'extérieur des frontières nationales présente donc un danger pour la « *normalité* », sinon plus encore la « *loyauté* » des citoyens envers la Nation ; quand le but sera moins de conserver les « *biens personnels et l'intégrité de personnes en particulier* », que de « *préserver l'ordre public* » dans sa globalité appelant comme réponse particulière non pas la « *réglementation* », mais plutôt l' « *état d'exception* ». A cet égard, l'exemple du plan « *vigipirate : alerte attentat* » en témoigne : s'il est théoriquement un dispositif exceptionnel, il reste aujourd'hui permanent[240] et fait craindre l'exercice d'une sécurité policière politique prolongé (*Voir tableau schématique des différents modèles contemporains de sécurité en annexe II.)*

Section II : Atteintes visant à recueillir, soustraire des informations sensibles

Les atteintes à l'ordre public peuvent aussi porter sur l'espionnage et le trafic clandestin : dans un contexte de mondialisation, elles sont autant d'actualité que le phénomène terroriste (*Sous-section I*), tandis que leur impact est non seulement économique, mais aussi militaire. Si elles concernent autant la sécurité policière que militaire, elles ont de commun leur nature essentiellement politique (*Sous-section II*).

[238] A cet égard, les attentats commis contre les ambassades américaines de Nairobi et de Dar-es-Salam le 7 août 1998 ont tué 213 personnes et fait 4 000 à 5000 blessés : si seulement 12 personnes tuées étaient américaines, le reste des victimes blessées ou tuées étaient de confession musulmane.

[239] On peut prendre l'exemple de « *terroriste internes* » comme Mohammed Mera, les frères Kouachi, ou le normand Maxime Hochard.

[240] MARCHAND Leila, « *Plan Vigipirate : comment un dispositif exceptionnel est devenu permanent* », Le Monde, 24 avril 2014.

§.1/ Le recueillement d'informations sensibles, un vecteur d'espionnage contemporain.

Les atteintes visant à recueillir, soustraire des informations sensibles se distinguent de celles commises à des fins de diffusion d'informations, de propagande car elles visent cette fois principalement à récolter frauduleusement des informations confidentielles, à des fins concurrentielles notamment.

L'éditeur de logiciels de sécurité « *McAfee* » relevait déjà en 1994 que les ordinateurs du Département de la Défense Américaine auraient été visités plus de 300 000fois par des inconnus, avant que la section du département américain du commerce ne soit piratée en 2006. En Europe, c'est la Grande Bretagne qui fût l'objet d'atteintes similaires, tandis que selon les estimations de l'éditeur de logiciels, 300 agences gouvernementales et entreprises auraient été la cible d'attaques visant à accéder de manière frauduleuse à des informations confidentielles[241].

Face à ces menaces, le législateur national est donc intervenu : la loi du 26 juillet 1986[242] incrimine désormais le fait de communiquer à des autorités publiques étrangères, des renseignements d'ordre économique, commercial ou industriel, financier ou technique de nature à porter atteinte à la souveraineté ou aux intérêts économiques essentiels de la France. Ces actes sont notamment punis de six mois d'emprisonnement et 18 000euros d'amende.

Parallèlement, les articles 411-6 et suivants du code pénal sont venus incriminer le fait de livrer à une puissance les informations de nature à porter atteinte aux intérêts fondamentaux de la Nation, tandis que ces opérations d'espionnage peuvent être qualifiées au travers de plusieurs infractions :

Il peut s'agir de la violation de correspondance et de communication électronique[243], de la commercialisation illicite d'appareils conçus pour intercepter les communications électroniques ou conversations, et même de la publicité pour ces appareils[244]. L'infraction classique d'accès frauduleux à un système informatique[245] trouve là encore à s'épanouir d'ailleurs : la peine sanctionnant le recel de l'infraction est notamment aggra-

[241] http://www.macafee.com/us/local-content/reports/mcafee-criminology-report2007-en.pdf.
[242] Loi n°68-678 du 26 juillet 1986.
[243] Article 226-15 et -31 du code pénal : « *est puni d'un an d'emprisonnement et de 45 000eros d'amende, le fait pour une personne d'avoir ouvert, supprimé, retardé ou détourné des correspondances adressées à des tiers, ou frauduleusement pris connaissance de celles-ci, [ou d'avoir] intercepté, détourné, utilisé ou divulgué des correspondances émises, transmises ou reçues par voie de télécommunications, et ce au préjudice de la victime*. »
[244] Article 226-3 du code pénal : « *est puni de cinq ans d'emprisonnement, et de 300 000euros d'amende, le fait pour une personne de commercialiser sans autorisation ministérielle, y compris par négligence, fabriqué, importé, détenu, exposé, offert, loué ou vendu un appareil ou un dispositif technique conçu pour intercepter, détourner, utiliser ou divulguer des correspondances émises, transmises ou reçues par la « voie électronique », ou de l'avoir conçu pour la détection à distance des conservations, permettant de capter, d'enregistrer ou de transmettre, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel. Les mêmes peines sont applicables à la publicité en faveur de ces appareils, dispositifs techniques susceptibles de permettre la réalisation d'atteintes à la vie privée*. »
[245] Article 323-1 et s. du code pénal : « *est puni de deux ans d'emprisonnement et de 30 000euros d'amende, le fait d'accéder, ou de se maintenir en tout ou partie dans un système de traitement automatisé de données*. »

vée lorsqu'il s'agit d'un accès, ou maintien frauduleux dans un système de traitement mis en œuvre par l'Etat depuis la loi du 27 mars 2012[246].

Enfin, concernant plus particulièrement le monde de l'entreprise, les attaques informationnelles commises à l'encontre des entreprises nationales peuvent aussi être constatées par le biais de la violation du secret professionnel avec divulgation, par l'une des parties, des informations concernant une autre partie ou un tiers dont elle n'a pu avoir connaissance qu'à la suite des communications ou consultations auxquelles il a été procédé dans le cadre des attributions de l'Autorité de la concurrence[247].

§.2/ Le recueillement frauduleux d'informations sensibles, un impact économique significatif sur le principe de sécurité militaire :

L'actualité des menaces d'espionnage concerne aujourd'hui moins la pérennité des entreprises[248], que la survie de l'Etat dans un contexte mondialisé :

Les révélations sur les programmes d'espionnage menés par la NSA ont entraîné des « *(...) changements fondamentaux et irréversibles dans beaucoup de pays et quantité de domaines* » selon le journaliste du Guardian[249] qui a rendu publiques les informations confidentielles recueillies par M. Edward Snowden. C'est que depuis 1950, les Etats-Unis disposent d'un réseau de surveillance globale qui, au gré des changements géopolitiques, a changé de fonction :

S'il était classiquement question « *d'équilibre les menaces* », dans le but de privilégier « *le principe d'indiscutable* » d'une position sur l'autre dans un contexte de guerre froide, afin de « *dissuader* » l'adversaire, de disposer d'hégémonie dans une « *sphère d'influence* » toujours plus étendue[250] , d'assurer *in fine* la sécurité militaire, cette surveillance va progressivement changer de fonction[251] :

Aujourd'hui, elle visera toujours à « *combattre les menaces, actuelles ou futures (...) pesant sur une économie mondiale construite autour des intérêt américains (...)»* mais va se diversifier *:* elle *[concernera désormais] les acteurs non étatiques, les pays moins développées bien déterminés à se faire une meilleure place dans l'économie mondiale ou, au contraire, les pays désireux de s'engager sur d'autres voies de*

[246] Loi n°2012-410 du 27 mars 2012.
[247] Article L.463-6 du code de commerce.
[248] Voir i*nfra*…Partie II, Titre I, Chapitre I, Section I
[249] Mr. Glenn Greenwald
[250] Dans le contexte de guerre froide, on parlera notamment de « *Etats-satellites* » du bloc occidental, notamment les pays d'Amérique latine et européens, ou soviétique avec notamment les républiques socialistes ou certains pays du proche orient ou d'Amérique latine.
(voir. *Op.Cit* « *Histoire du XXème siècle : le monde entre guerre et paix* ».)
[251] Voir *infra*... annexe II : les différents modèles de sécurité contemporaine.

développement, et […] d'autre pays capitalistes développés »[252]. Pour remplir ces nouveaux objectifs, l'industrie de la cyber guerre va se développer et donner lieu à des privatisations massives : ce qui était de longue date une fonction régalienne, dans un contexte de sécurité militaire, va se transformer en entreprise menée par l'Etat et les milieux d'affaires, visant moins à assurer une sécurité, qu'à réellement asservir les autres acteurs économiques étatiques ou non, alliés ou ennemis selon les circonstances et les changements de politique globale.

A ce titre, les acteurs de la sécurité sont aujourd'hui moins les gouvernements, que les multinationales disposant de technologies numériques de pointe[253] : la sécurité constitue moins le préalable classique nécessaire au développement de l'économie, que la résultante d'accords économiques internationaux permettant aux gouvernements qui en usent, d'asseoir leur position stratégique sur un marché. Dès lors, les fruits de l'obtention d'un marché leur permettront non seulement de développer leur influence sur le terrain géopolitique, mais encore de nourrir leur influence militaire sur les autres acteurs de la scène internationale.

Section III/ Risques liés aux atteintes informationnelles

Les deux types d'atteintes, selon qu'elles visent à diffuser ou à recueillir des informations sensibles suscitent des réponses adaptées des pouvoirs publics, qu'elles visent à assurer la sécurité politique à l'intérieur du territoire, ou militaire visant l'extérieur des frontières cette fois : cependant, elles ont de commun leur faculté de tempérer le principe de liberté de l'Internet (*Sous-section I*), leur impact privilégiant la souveraineté d'Etat, sur celle de l'individu (*Sous-section II*).

§.1/ Risques pour le principe de liberté d'Internet

« *Internet donne à chacun d'entre nous la possibilité de s'exprimer, de créer, d'apprendre et de partager*[254] ». A ce titre, si l'Internet apporte une énorme contribution au développement, l'exercice de la liberté d'expression doit être sauvegardé et promu non seulement aux médias traditionnels, mais encore à « *(…) tous les types de plates-formes médiatiques émergentes contribuant au développement, à la démocratie et au dialogue* » selon le rapport de l'UNESCO, « *Freedom of Connection – Freedom of Expression* »[255].

---

[252] *Op.Cit*…« *Géopolitique de l'espionnage* » *Ibidem*….« *Le Monde Diplomatique* ».
[253] Voir i*nfra*…Partie II, Titre I, Chapitre I, Section I.
[254] Déclaration de CERF Vinton, considéré comme l'un des pères fondateurs d'Internet avec l'ingénieur KAHN Bob ou le britannique BERNERS-LEE Tim : « *Nous devons défendre la liberté sur Internet, par Vinton* Cerf », « *Le Monde* », 4 décembre 2012.
[255] www.unesco.org : Communication et information, Thèmes, Liberté d'expression, Liberté d'expression sur Internet.

Cependant, on recense encore aujourd'hui plus de la moitié des pays privilégiant la censure des contenus sur Internet[256] : dans certaines régions du globe marqués par l'instabilité politique[257], l'un des moyens les plus efficaces de contenir les insurrections populaires consiste en effet à couper les connexions Internet, ou le réseau de téléphones mobiles afin de cloisonner les frontières, et d'empêcher une circulation non seulement libre, mais encore neutre, pouvant constituer une critique des autorités publiques en place[258]. Cette neutralisation du réseau Internet, garantie d'une liberté d'expression et de l'information, est d'ailleurs privilégiée de longue date par certains régimes politiques qualifiés d'autoritaires, comme celui de la Corée du Nord : le système repose sur une forme d'intranet ouvert permettant d'accéder à des sites d'information coréens, à la télévision éducative et à des formes rudimentaires de boite e-mail, quand ces outils sont utilisés majoritairement par les habitants de la capitale. Par ailleurs, la possession d'un ordinateur doit nécessiter une autorisation officielle, tandis que les Nord-Coréens pouvant accéder au réseau intranet, ne pourront téléphoner qu'à l'intérieur des frontières du pays, à la condition qu'ils reçoivent quotidiennement des messages de propagande à la gloire du régime[259].

Le principe de liberté d'Internet peut donc constituer une menace pour la sécurité policière politique, car s'il permet d'ouvrir une fenêtre sur le monde, il implique nécessairement que le monde puisse voir au travers de cette fenêtre : à ce titre, il peut menacer la « *préservation de l'ordre public* », tel qu'entendu par le régime politique en place, qu'il consiste à asseoir une légitimité[260] ou à préserver une idéologie[261] et justifie le maintien de l'ordre. Or, si l'ordre peut être assuré par la force, il découle nécessairement d'une « *domestication* » des comportements déviants, lesquels trouvent particulièrement matière à s'épanouir sur le terrain de l'Internet, dès lors qu'ils pourront « *contaminer* » d'autres souches de la population, ce qui présente un risque pour l'intégrité d'un régime politique en place. La censure permettra donc d'asseoir une « *loyauté* » sur l'ensemble, permettant d'éradiquer la déviance menaçant le régime, et de promouvoir la « *dénonciation* » de ces comportements, afin de contenir les risques de contamination, donc de propagation de la critique à l'encontre du régime. (*Voir les différents modèles contemporains de sécurité en annexe II*.)

[256] Selon une étude de l' « *Open Net Initiative* », 42 pays filtrent et censure des contenus sur Internet, sur un ensemble de 72 pays étudiés.
[257] On peut par exemple prendre aujourd'hui la Syrie
[258] Selon une étude menée par «*Amnesty International* », les autorités syriennes auraient cherché à empêcher le monde d'apprendre ce qui l'évolution de la situation depuis 2012, dans un contexte d'intensification des combats à Damas entre le régime de Bachar El Assad et les forces révolutionnaires syriennes.
[259] « *Que sait-on de l'Internet en Corée du Nord* », bloggeur « *BigBrowser* », « *Le Monde* », 23 décembre 2014.
[260] Bachar-El-Assad combat les forces révolutionnaires afin d'asseoir l'autorité de son régime par exemple.
[261] Kim Jong-Un interdit toute relation avec l'extérieur dans le but de préserver l'idéologie communiste sur le territoire par exemple.

§.2/ Risques pour le principe de « sécurité humaine ».

« *La sécurité humaine pourrait offrir une nouvelle approche de la sécurité et du développement : elle concerne la sécurité des individus et des communautés plus que celle des Etats*[262] » :

Comme le rappelle le Programme des Nations Unies pour le Développement (PNUD) de 1994, « *le concept de sécurité (…) s'applique davantage aux Etats-Nations qu'aux personnes* », le principe de sécurité humaine visera dès lors moins à insister sur la sécurité de l'Etat, que sur celle de l'individu, privilégiant la sécurité sur la violence politique. L'assise du principe contemporain de sécurité humaine serait plus que jamais nécessaire aujourd'hui, tandis que le développement des technologies de l'information et de la communication conduit l'ensemble de la population du globe à prendre connaissance des souffrances endurées par certains peuples, dans certaines régions ; par ailleurs, tandis qu'au lendemain de la Seconde Guerre Mondiale, les Etats en adhéré à une série de conventions, traités et déclarations, l'abolition des frontières traditionnelles conduirait plus encore les Etats à respecter leurs obligations.

Cependant, les atteintes informationnelles peuvent porter un coup d'arrêt à l'exercice de ce nouveau principe de sécurité humaine : c'est que les atteintes visant à diffuser, propager des informations sensibles, conduisent de plus en plus les Etats à recourir à une violence politique, plutôt qu'à assurer la sécurité. A cet égard, tandis que le terrorisme constitue une notion protéiforme et évolutive, il vise avant tout à promouvoir une idéologie politique aux antipodes de celle défendue par l'Etat : il s'agit par exemple de la politique indépendantiste promue par le Groupe Islamiste Armé (GIA) qui s'insurge contre le pouvoir algérien dans le but d'établir un gouvernement islamiste, ou d' « *Al Qaeda* » ou « *Daech* » qui poursuivent une même logique, opposée aux conceptions occidentales de l'Etat de droit.

On retrouve par ailleurs une illustration de cette violence politique avec le nouveau délit d'apologie du terrorisme[263], lequel peut moins constituer une apologie de la violence à proprement parler, que la défense d'une position idéologie opposée à celle promu par le gouvernement français. Il s'agit dès lors moins de promouvoir la sécurité juridique de l'individu que celle policière de l'Etat, impliquant la défense du gouvernement. La radicalisation de certains occidentaux traduit d'ailleurs cette logique de « *souveraineté de l'Etat*» : bien que ces derniers soient nés, et aient grandi à sur le territoire national, ils peuvent marquer leur rejet des positions prises par l'Etat sur la scène internationale en critiquant la prévalence des intérêts du gouvernements sur ceux des populations opprimées : il s'agira alors moins pour l'Etat de sauvegarder une certaine liberté d'expression, que de s'assurer de la loyauté de ces derniers au gouvernement, de conforter une sécurité juridique plutôt que de promouvoir une police politique.

---

[262] KALDOR Mary, « *La sécurité humaine : un concept pertinent ?* », Institut Français des Relations Internationales, Politique Etrangère, hiver 2006, 350 pp.

[263] Voir *infra*… Partie I, Titre III, Chapitre III, Section I

TITRE II / Des réponses réelles face à des menaces virtuelles :

L'actualité de ces nouvelles menaces numériques suscite notamment de nouvelles dynamiques étatiques (**Chapitre I**) : il s'agit non seulement de développer de nouveaux dispositifs de sécurité, mais encore de renforcer les mesures contraignantes classiques (**Chapitre II**), ce qui n'est pas sans soulever de nouvelles problématiques de société quant à l'exercice de l'activité de l'Internet aujourd'hui (**Chapitre III**.)

Chapitre I :
Dynamiques étatiques

Plusieurs réponses se développent face à l'émergence des nouvelles menaces numériques : celles-ci résultent notamment de l'après 11 septembre 2001 au niveau international, et impliquent des conséquences au niveau régional (***Section I***). Elles nécessitent alors un contrôle de la part d'organisations intergouvernementales, comme en témoignent les initiatives prises par le Conseil de l'Europe ou la Communauté Européenne, visant à préserver la protection d'une sécurité juridique globale des particuliers (***Section II***).

Section I / Dynamiques internationales

A la suite des attentats du 11 septembre 2001, une surveillance générale a été institutionnalisée (*Sous-section I*), tandis que les événements survenus en début d'année 2015 font craindre une résurgence de dispositifs similaires au niveau européen (*Sous –section II*).

§.1/ L'après 11 septembre 2001, ou la surveillance de masse

Suite aux attentats du « *Walt Trade Center* », les autorités américaines ont pris un texte de loi dont le principal objectif consistait à effacer la distinction juridique entre les enquêtes effectuées par les services de renseignement extérieur, notamment la « *Central Intelligence Agency* » (CIA), et celles menées par le « *Federal Bureau of Investigation* » (FBI), en créant notamment une nouvelle catégorie de comportement criminel : « *le terrorisme intérieur* »[264].

Ce texte de loi permettait notamment plusieurs mesures très intrusives dans la vie privée des ressortissants américains suspectés de préparer des actes de terrorisme : le FBI et le département de la Justice pouvaient utiliser certaines dispositions du texte afin d'accéder notamment aux fichiers de lecteurs des bibliothèques et libraires, ou d'effectuer des perquisitions en l'absence même de la personne concernée par la mesure. Cependant, l'objet phare du texte était contenu dans le titre relatif aux « *Enlèvement des obstacles sur*

[264] Section 802 du « *USA Patriot Act* ».

l'investigation dans le terrorisme », et réformait le « *Foreign Intelligence Surveillance Act* » de 1978 qui organisait les procédures de surveillance physiques et électroniques concernant les puissances étrangères seulement :

Le « *Patriot Act* » de 2001 prévoyait désormais que le FBI puisse obliger les fournisseurs d'accès à internet à permettre de leurs bases de données personnelles, tout en leur interdisant d'informer les personnes ciblées de la transmission de leurs données aux autorités : les personnes ciblées n'étaient plus seulement celles soupçonnées de terrorisme ou d'espionnage, mais bien l'ensemble de la population américaine. Par ailleurs, toute entreprise était désormais tenue de fournir ces données sensibles réclamées par l'administration fédérale, même si ces dernières étaient stockées en Europe. Un dispositif similaire et conjoint au « *Foreign Intelligence Surveillance Act* » fût par la suite été déployé pour permettre cette fois à la « *National Security Agency* » (NSA) de contribuer à cette surveillance de masse, mais à l'extérieur des frontières américaines cette fois : on appelle ce dispositif, le « *Terrorist Surveillance Program* » (TSP).

Ce nouvel outil législatif permettait à l'agence de sécurité nationale américaine de surveiller, sans mandat judiciaire, les appels téléphoniques, les courriels ainsi que l'ensemble de l'activité Internet s'il existait des indices laissant supposer que l'un des interlocuteurs soupçonnés de préparer des actes de terrorisme se trouvait à l'extérieur des frontières étatsuniennes. L'outil consacraient donc de nouveaux pouvoirs intrusifs, mais surtout pris en violation du « *Wiretap Act* », lequel interdisait à toute personne d'intercepter ou de publier des communications électroniques ou téléphoniques[265].

L'esprit du « *Patriot Act* » a mécaniquement suscité de nombreuses réactions dans la société civile : à cet égard, c'est notamment l' « *Union Américaine pour les Libertés Civiles* » (ACLU) qui, loin de se contenter de critiques publiques quant au caractère liberticide du « *Patriot Act* » à l'égard du principe de respect de la vie privée et de liberté d'expression, a notamment poursuivi en justice la NSA en alléguant de l'inconstitutionnalité du TSP. Elle fût cependant déboutée pour des motifs de « *secret d'Etat* » (« *Privilege Secret State* ») prohibant tout droit de l'ACLU de se pourvoir en justice, c'est dire que les circonstances conduisaient à privilégier la « *raison d'Etat* » sur les libertés citoyennes, l'exercice d'une sécurité policière sur l'exercice d'une sécurité juridique.

[265] Titre 18, Section 2511 relatif aux « *Interceptions d'écoutes, de paroles, ou de communications électroniques* »

§.2/ L'accord PNR UE- Etats Unis

En 2012, l'accord « *Passenger Name Records* » sur les données des passagers aériens a été adopté par 409 voix pour, 226 voix contre et 33 abstentions parle Parlement Européen[266] :

Depuis 2007[267], l'accord relatif au traitement et au transfert de données des dossiers passagers par les transporteurs aériens au ministère américain de la sécurité intérieure avait été pris par décision du Conseil : il s'agissait alors des données relatives aux informations anticipées sur les passagers comme le nom, le sexe, la civilité, la date de naissance ou le pays de résidence ; des informations relatives au voyage, faisant figurer la date de réservation ou d'émission du billet, la date du voyage, l'itinéraire ou le statut du voyageur ; ou concernant le billet d'avion, indiquant si celui-ci était gratuit ou surclassé. Au-delà de ces informations générales, les données pouvaient concerner des domaines plus sensibles : elles visaient à révéler notamment l'origine ethnique, les opinions philosophiques, politiques, syndicales ou la santé et la vie sexuelle de l'individu. Or, depuis l'entrée en vigueur du Traité de Lisbonne, la décision cadre relative au transfert des données des dossiers passagers devenait caduque, et nécessitait le développement d'un nouveau cadre législatif :

C'est ce qu'ambitionnait de faire la directive présentée le 2 février 2001 par la Commission européenne qui reprenait les grandes lignes fixées en 2007, tout en modifiant certains dispositifs comme le temps de conservation des données, dorénavant de trente jours, ou cinq ans sous conditions d'être au préalable « *anonymisées* » ; en supprimant la possibilité de récolter, conserver des données à caractère sensible, telles que celles intéressant la sphère confessionnelle, ou politique du voyageur ; en développant enfin une méthode conduisant les transporteurs aériens à exporter les données, empêchant les autorités répressives d'extraire de leur propre chef ces données. Cependant, malgré ces ajustements, la Commission des libertés civiles du Parlement européen rejeta l'application de cette directive qui présentait un « *caractère intrusif pour les voyageurs innocents* », dont l'utilisation proactive s'apparentait à un profilage méconnaissant le principe de proportionnalité contenu à l'article 8§2 de la Conv.EDH[268], dans une décision du 24 avril 2013.

Malgré tout, face à la résurgences des menaces liées au phénomène terroriste, plusieurs Etats membres se sont dotés d'un système de « *PNR* » comme le Royaume-Uni, la France, le Danemark ou la Suède : face aux nécessités d'harmoniser le régime juridique applicable au traitement de ces données au niveau européen,

---

[266] « *Le Parlement européen donne son feu vert à l'accord PNR avec les Etats-Unis*», Actualité, Parlement Européen, 19 avril 2012.
www.europarl.europa.eu

[267] Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007, relative à la signature au nom de l'Union Européenne et les Etats Unis d'Amérique sur le traitement et le transfert des dossiers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure.

[268] Le principe de proportionnalité a été dégagé la première fois par la CEDH dans l'arrêt « *Marper c/Royaume Uni* » du 4 décembre 2008.

combiné à l'intervention croissante de la Communauté Européenne en matière de protection des données personnelles[269], le Parlement européen a finalement manifesté sa volonté de parvenir à un accord « *PNR* » qui, non content d'assurer seulement un contrôle des flux de voyageurs, viendrait par ailleurs assurer une protection juridique homogène et uniforme sur le plan européen[270].

Quand l'exercice d'une sécurité policière s'imposa pour les Etats membres, la mission du Conseil de l'Europe consistait à développer un cadre juridique global assurant un minimum de sécurité juridique aux citoyens européens.

Section II / Dynamiques européennes

Le Conseil de l'Europe s'est illustré en matière de contrôle du principe de protection des données personnelles avec la Convention 108 (*Sous-section I*), quand la Communauté Européenne emboîte le pas, et illustre l'ancrage d'une protection des données personnelles dans le « *cyberespace* » européen (*Sous-section II*).

§.1/ Coopération européenne en matière de lutte contre les menaces numériques : la Convention 108 du CE.

La Convention 108 du CE[271] était et reste aujourd'hui, le seul acte à force juridique obligatoire internationale dans le domaine de la protection des données[272] :

Dès le milieu des années 1970, le Comité des Ministres du CE a adopté plusieurs résolutions concernant la protection des données personnelles, avant de soumettre la Convention 108 à ratification des Etats membres. Cette Convention s'applique aujourd'hui à tout traitement de données à caractère personnel, qu'il implique le secteur privé ou public, et concernera autant les autorités judiciaires que celles chargées d'appliquer la loi. Outre la protection qu'elle instaure à l'égard des abus susceptibles d'être commis dans la collecte et le traitement des données à caractère personnel, la Convention 108 énonce notamment des principes visant à établir une collecte licite et loyale, un traitement automatisé des données conservées à des fins légitimes définies. Les principes visent par ailleurs la qualité des données, lesquelles doivent être adéquates, pertinentes, proportionnelles et exactes.

---

[269] Voir *infra*….Section II, Sous-section II.
[270] « *Le Parlement européen négocie son engagement sur le PNR européen* », Euractiv.com, L' « *Europe dans le monde* », News, 25 février 2015.
[271] La Convention 108 du CE a été adoptée le 28 janvier 1981.
[272] « *Manuel de droit européen* », Agence des droits fondamentaux de l'Union européenne, avril 2014, Conseil de l'Europe, p.16 et ss.

Par-delà ces principes généraux, certaines interdictions sont posées, notamment celles visant à prohiber le traitement de données "*sensibles*", telles que l'origine raciale, l'opinion politique, l'état de santé, les convictions religieuses, la vie sexuelle ou les condamnations pénales d'une personne. Parallèlement, il s'agira alors de concilier la libre circulation des données à caractère personnel entre Etats membres, avec la restriction de circulation susceptible de conduire ces données à destination d'un Etat dont la réglementation ne prévoirait pas de protection appropriée.

La Convention 108 ne garantirait pas seulement le principe de protection des données personnelles, en adéquation avec les dispositions de l'article 8 de la Conv.EDH, mais tendrait plus encore à ériger un contrôle réel au niveau européen. Ce contrôle s'est notamment étendu au territoire communautaire depuis 1999[273], et vise à s'appliquer à terme à l'international : dans cette optique, certaines dispositions sur les flux transfrontières de données vers des pays n'étant pas parties à la Convention 108 ont notamment été introduites par le Protocole additionnel de 2001.

Comme le relève le "*Manuel de droit européen en matière de protection des données*" de 2014, la Convention 108 aujourd'hui ouverte à l'adhésion des Etats non-membres du CE, qu'ils soient européens ou non, pourrait à l'avenir constituer une norme universelle de base à la promotion de la protection des données au niveau mondial. A cet égard, si en 2013 le premier pays non européen a adhéré à cette Convention[274], c'est le Maroc qui aujourd'hui formalise son adhésion.

§.2/ L'ancrage d'une protection des droits et libertés fondamentaux dans le « cyberespace », traduction dans le droit de l'UE :

Le principal acte juridique de l'UE est la directive 95/46/CE du Parlement européen et du CE du 24 octobre 1995. Outre la décision du 13 mai 2014[275], c'est sur son fondement que la Grande Chambre (GC) de la CJUE a rendu en avril 2014[276] un arrêt "*invalidant*" la directive européenne sur la conservation des données électroniques adoptée en mars 2006[277].

La directive 95/46 vise selon la CJUE "*à rendre équivalent dans tous les Etats membres le niveau de protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel[…][Tandis que le] rapprochement des législations nationales applicables en la matière ne doit*

[273] Le 15 juin 1999, des amendements à l'article 23, §.2 de la Convention 108 ont été adoptés par le Comité des Ministres, à Strasbourg, afin de permettre aux Communautés européenne d'y adhérer.
[274] L'Uruguay.
[275] Voir *infra*...Partie I, Titre III, Chapitre II, Section III, Sous-Section II.
[276] CJUE, GC, arrêt du 8 avril 2014, "*Digital Rights Ireland Seitlinger e.a*", n°94/2014.
[277] Directive du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de service de communications électroniques accessibles au public ou de réseaux publics de communications.

pas conduire à affaiblir la protection qu'elles assurent, mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'Union […]. Ainsi, […] l'harmonisation des dites législations nationales ne se limite pas à une harmonisation minimale, mais aboutit à une harmonisation qui est, en principe, complète"[278]. Cette directive a notamment été conçue pour consolider les principes du droit à la vie privée déjà contenus dans la Convention 108, tandis que son application s'étend au-delà des 28 Etats membres de l'UE et inclut les Etats membres de l'Espace économique européen comme l'Islande, le Liechtenstein et la Norvège.

Cependant, la directive présentait certaines lacunes au niveau de son application territoriale et matérielle. Concernant l'application territoriale, elle ne concernait pas les institutions et organes communautaires : le Parlement européen et le Conseil ont dû prendre alors le règlement (CE) n°45/2001 concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel par ces institutions et organes. Par ailleurs, concernant cette fois l'application matérielle, certaines directives supplémentaires ont été prises afin de couvrir non seulement la protection de la vie privée dans le secteur des communications électroniques[279], mais encore dans le domaine cette fois des services de communications électroniques accessibles au public[280], avant que cette dernière ne soit cependant invalidée par décision de la Grande Chambre (GC) de la CJUE.

Parallèlement, c'est la Charte des droits fondamentaux de l'Union européenne ayant acquis force obligatoire avec l'entrée en vigueur du Traité de Lisbonne de 2009 qui garantit le droit au respect de la vie privée et familiale[281], comme le droit à la protection des données[282] au niveau de l'UE, traduisant les initiatives de la Communauté européenne en matière de protection des libertés personnelles, notamment de la vie privée des citoyens européens sur le terrain numérique.

Cependant, si la Commission européenne appelle depuis 2012 à une modernisation de la directive 95/46/CE au regard des évolutions technologiques rapides et de la mondialisation, il s'agirait principalement de développer une nouvelle directive relative à la protection des données dans le domaine notamment de la coopération policière et judiciaire[283] aujourd'hui, de mettre l'accent sur le développement d'une sécurité policière pour l'avenir.

---

[278] *Op.Cit..."Manuel de droit européen en matière de protection des données" Ibidem...*p.18 et ss.
[279] "*Directive vie privée et communications électroniques*", n° 2002/58/CE
[280] "*Directive sur la conservation des données*" n°2006/24/CE
[281] Article 7 de la Charte des droits fondamentaux de l'Union européenne
[282] Article 8 de la Charte des droits fondamentaux de l'Union européenne.
[283] *Op.Cit ..."Manuel de droit européen en matière de protection des données" Ibidem...*p.21 et ss.

Section III / Dynamiques nationales

Le projet de loi sur le renseignement de février 2015 ne constitue pas une loi « *post-Charlie* » malgré ses apparences : son origine remonte à une condamnation de la France par la CEDH (*Sous-section I*), quand la réflexion autour d'un cadre juridique relatif aux activités de renseignement se dessinait dès 2013 (*Sous-section II*). Aujourd'hui, ce projet résulte donc plus d'une réflexion arrivée à maturation, que d'une réponse structurelle aux événements récents (*Sous-section III*).

§.1/ L'origine : la loi sur les interceptions téléphoniques du 10 juillet 1991

Le régime juridique applicable à la protection des données personnelles sur le territoire national résulte directement de la condamnation de la France par la CEDH dans l'affaire "*Kruslin c/ France*" du 24 avril 1990[284] : en l'espèce, le placement sous écoute téléphonique par un juge d'instruction dans le cadre d'une affaire d'assassinat violait l'article 8 de la Conv.EDH, en l'absence de "(…) *clarté suffisante pour déterminer l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans ce domaine*.".

Comme le révèle l'ancien officier de police Georges Moreas, la circulaire du 28 mars 1960 classée secret-défense, prévoyait déjà la création d'un Groupement Interministériel de Contrôle (GIC) chargé de "*l'ensemble des écoutes et enregistrements téléphoniques et télégraphiques sur fils ainsi que des renvois sur réseau PTT des écoutes microphoniques, ordonnées par les autorités gouvernementales (...) [Il] disposait alors (...) des installations d'écoutes et d'enregistrements existant dans les différents ministères et services pratiquant actuellement des interceptions téléphoniques*." Or, si le groupement placé alors sous l'autorité directe du Premier ministre centralisait au niveau national toute les demandes d'interceptions administratives présentées les différents services habilités, les techniques de recueil des renseignements utilisées dans le cadre des écoutes se sont logiquement modernisées afin de s'adapter aux évolutions technologiques de la société : les interceptions ont alors été étendues au domaine de la téléphonie mobile, aux SMS, ou à l'Internet[285] au fil des années…

Parallèlement, dans le domaine judiciaire cette fois, les écoutes étaient prises sur le seul fondement de l'article 81 du code de procédure pénale, lequel dispose seulement que "*le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité*". Le flou qui entourait le cadre légal applicable aux écoutes conduisait généralement les enquêteurs ou les magistrats à

[284] Arrêt "*Kruslin c/ France*", CEDH, 24 avril 1990, n°11801/85.
[285] MOREAS Georges, "*Ecoute et espionnage : les Français sous surveillance*", article du 15 décembre 2013, www.moreas.blog.lemonde/2013/2015/ecouts-et-espionnage-les-francais-sous-surveillance/

utiliser la technique de la "*boîte vide*"[286] : le procédé consistait à utiliser une procédure destinée à être classée sans suite, et à y introduire un dispositif d'écoute qui concernait une autre affaire dans laquelle des personnes pouvaient être mises en cause. La technique méconnaissait ainsi, non seulement les droits de la défense (le droit au procès équitable, ou de disposer des facilités nécessaires à la préparation de sa défense...) mais plus encore, le principe de prévisibilité de la loi pénale contenu à l'article 7 de la Conv.EDH[287], transposé à l'article 111-4 du code pénal[288].

Devant ce flou juridique entourant les interceptions téléphoniques dans le domaine administratif comme judiciaire, la condamnation de la France par le juge européen a conduit le législateur à prendre un texte législatif : la loi du 10 juillet 1991[289]. Désormais, la loi justifiaient les écoutes administratives "*dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celles-ci*", quand son article 2 encadrait les écoutes judiciaires, lesquelles ne pouvaient être déclenchées qu'"*en matière criminelle et en matière correctionnelle, si la peine encourue était égale ou supérieure à deux ans d'emprisonnement*".

§.2/ La réflexion : le rapport parlementaire sur l'évaluation du cadre juridique applicable aux services de renseignement de 2013.

Le projet de loi sur le renseignement ne constitue pas un texte "*post Charlie*"[290], il est plutôt le fruit d'une réflexion amorcée deux années plus tôt. En 2013, la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République prenait un rapport d'information en conclusion des travaux d'une mission sur l'évaluation du cadre juridique applicable aux services de renseignement[291] :

Ce rapport établi par les députés Jean Jacques Urvoas et Patrice Verchère proposait déjà qu'une loi soit prise pour légitimer et encadrer les activités de renseignement (première partie), avant de se pencher notamment sur la nécessité de repenser la coordination et d'adapter l'organisation des services (deuxième partie). Concernant la nécessité de créer un cadre juridique protecteur des intérêts fondamentaux de la nation, l'ambition des auteurs du rapport tendait à inciter au développement de nouveaux moyens légaux à

[286] La technique de la "*boîte vide*" est illustrée dans la fiction, notamment dans la série américaine "*the wire*" ("*sur écoute*") ou des enquêteurs créent de toute pièce une tueur en série de SDF dans le but d'obtenir des fonds, et notamment un dispositif d'écoute qui leur permettrait d'identifier et d'interpeller ce suspect imaginaire : les enquêteurs se servent du dispositif pour arrêter un trafiquant de drogue qu'ils placent sur écoute, tandis que ce dernier n'était pas visé par l'enquête judiciaire.
[287] L'article 7 de la Conv.EDH proclame le principe selon lequel il n'y a "*Pas de peine sans loi*".
[288] L'article 111-4 du code pénal dispose que "*La loi pénale est d'interprétation stricte*".
[289] Loi n°91-646 du 10 juillet 1991.
[290] L'expression fait référence aux attentats ayant frappé le siège de la rédaction du journal satirique "*Charlie Hebdo*" en janvier 2015, lesquels furent suivis d'une manifestation le 11 janvier 2015 dont le mot de ralliement était "*Je suis Charlie*". Par la suite, en réaction au projet de loi sur le renseignement, plusieurs médias (*"Le Monde","Slate", "Legrandsoir", "Agoravox"*…) ou personnalités (Edward Snowden notamment) ont parlaient d'une loi "*post-charlie*".
[291] Le rapport est disponible sur le site de l'Assemblée Nationale, à cette adresse : www.assemblee-nationale.fr/14/pdf/rap-info/i1022.pdf.

disposition des services de renseignement, devant les carences des trois moyens traditionnels actuellement utilisés par ces services (les interceptions de sécurité, les systèmes de réquisition des données techniques de connexion, les fichiers).

Les préconisations concernaient ainsi l'extension du dispositif d'infiltration prévu en matière de trafic de stupéfiants[292] aux activités de renseignement, notamment lorsqu'il existait des indices permettant de suspecter la préparation, par un groupe, d'une atteinte aux intérêts fondamentaux de la Nation, à la sécurité nationale ou à la forme républicaine du Gouvernement. Il proposait par ailleurs une clarification du dispositif de géolocalisation en temps réel qui apparaissait déjà justifiée à l'époque[293]..

Surtout, le rapport proposait d'autoriser de nouveaux procédés qui permettrait de s'adapter à l'évolution des technologies : ainsi, "*lorsque la personne cible change par exemple sans cesse de numéro de téléphone, l'interception de sécurité se révèle tout à fait inutile (...), il pourrait être judicieux d'autoriser le recours à un outil aujourd'hui exploité par des officines privées œuvrant dans la plus parfaite illégalité, dit "IMSI catcher*" : aujourd'hui, c'est l'article 2 du projet de loi sur le renseignement qui consacre notamment l'utilisation de ce dispositif[294].

§.3/ La maturation : le projet de loi sur le renseignement de 2015

Le Premier Ministre Français a présenté le jeudi 19 mars 2015 le projet de loi relatif au renseignement, il s'agissait de pallier aux faiblesses de la France dans le domaine ou elle « *(...) constitue l'une des dernières démocraties occidentales à ne pas disposer d'un cadre légal, cohérent et complet pour les activités de ses services de renseignement* »[295] :

Selon le Gouvernement, ce projet aurait pour but de donner aux services de renseignement les «*(...) moyens à la hauteur des défis auxquels notre pays est confronté (...) tout en visant à offrir plus de garanties pour les agents qui évoluant jusqu'ici dans un cadre juridique incertain ; [le projet de loi en consacrant] plus de garantie pour les libertés publiques [garantirait] donc plus de sécurité pour les Français* » : en ce sens, il reprendrait à l'exacte la doctrine politique amorcée dès la fin des années 1990, qui plus est par la même formation, selon laquelle la « *sécurité est une condition d'exercice des libertés* »[296], et s'inscrit donc dans la continuité d'une normalisation d'un cadre législatif encadrant les activités de renseignement. C'est en effet

[292] L'article 706-82 du code de procédure pénale dispose que l'infiltration consiste, pour l'agent ou l'officier de police infiltré "*à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs.*"
[293] Voir *infra*… Chapitre II, Section I, Sous-Section II.
[294] Voir *infra* ...Chapitre II, section II, sous-section II
[295] Site du Ministère de l'Intérieur, Accueil, Actualités, Dossier, Projet de loi sur le renseignement *www.interieur.gouv.fr/Actualités/Dossier/Projet-de-loi-sur-le-renseignement*
[296] Voir *infra*…. Premier article de la loi du 21 janvier 1995 relative à la vidéosurveillance

depuis 2006, que le Gouvernement a entrepris la démarche d'encadrement législatif du domaine relatif au renseignement, en créant notamment le Conseil national du renseignement, la fonction de coordonnateur national du renseignement en 2009, et la création de l'inspection des services de renseignement en 2014.

Le projet de loi viserait par conséquent à prévenir différents types de menaces : si la menace d'essence terroriste est principalement visée, la «*(...) France doit aussi se protéger contre l'espionnage, le pillage industriel, la criminalité organisée et contre la prolifération des armes de destruction massive* »[297]. Le renforcement des moyens d'action des services spécialisés de renseignement conduirait dès lors non seulement à garantir la sécurité des Français, mais aussi à préserver les intérêts fondamentaux de la Nation, à préserver la sécurité juridique des citoyens, comme celle politique de l'Etat de droit.

Ce projet s'inscrit alors dans un modèle policier hybride : s'il vise avant tout à « *préserver l'ordre public* », il conduit aussi à sauvegarder les intérêts fondamentaux de la Nation, tandis que lorsque l' « *Etat d'exception* » est privilégié sur le territoire national face à la survenance d'une menace, notamment par le « *renseignemen*t », l'exercice de la « *dissuasion* » permise par la récolte d'informations sensibles peut s'exercer à l'encontre des autres acteurs sur la scène internationale, et permettre de redessiner les « *sphères d'influences* » de chacun des acteurs : il viserait dès lors moins à identifier les citoyens « *déloyaux* » envers la Nation[298], qu'à défendre un « *alignement idéologique* », notamment occidental sur la scène internationale. Cependant, si la déloyauté peut entraîner la dénonciation[299], et tandis que l'"*alignement idéologique*" est classiquement promu par le principe d'indiscutable à l'extérieur[300] des frontières nationales, il menace de s'étendre progressivement à l'intérieur du territoire cette fois[301] (*Voir tableau schématique des différents modèles de sécurité contemporains en annexe II*.)

Chapitre II :

Moyens sécuritaires renforcés

Pour que la sécurité de l'activité d'Internet soit renforcée, de nouveaux dispositifs sont donc déployés au sein des services de police (***Section I***), comme des services de renseignement : ils assoient logiquement le principe de sécurité policière générale, voire politique dans nos sociétés, au détriment d'une sécurité juridique personnelle des particuliers (***Section II***).

---

[297] *Ibidem*…

[298] On peut citer par l'exemple les départs en Syrie,
voir infra… HAMAÏDE Julie, « *Le difficile retour en France des « repentis » du départ en Syrie* », 05 avril 2015, www.slate.fr

[299] Voir par exemple les plateformes de prévention de la radicalisation créées par le Ministère de l'Intérieur : www.stop-djihadisme.gouv.fr

[300] Voir par exemple la définition de l' « *axe du mal* » que donne l'ancien président des Etats Unis, George Bush, dans le « *Discours sur l'état de l'Union* », 29 janvier 2002.

[301] Voir *infra*… Partie I, Titre III, Chapitre III, Section I

Section I / Police

Si la police disposait déjà de moyens d'investigation spéciaux, mais finalement classiques (*Sous-section I*), de nouveaux moyens prometteurs, mais surtout intrusifs sont développés : ils visent logiquement à renforcer l'exercice d'une sécurité policière générale dans nos sociétés (*Sous-section II*).

§.1/ Les moyens d'investigation spéciaux, mais classiques

Les techniques spéciales d'enquête, réservées classiquement aux cas de criminalité organisée[302], ont été étendues aux nouvelles technologies du numérique : elles permettent dorénavant d'intercepter les conversations téléphoniques et électroniques, ou de capter les données informatiques.

Concernant les interceptions de correspondance, celles-ci étaient possibles dans le seul cadre d'une instruction[303] et ne concernaient que les infractions dont la peine encourue était égale ou supérieure à deux ans emprisonnement : ordonnées par un juge d'instruction pour une durée maximale de quatre mois, renouvelable dans les mêmes conditions de forme et de durée, elles étaient effectuées sous son autorité et son contrôle. Depuis 2004[304] cependant, ces interceptions peuvent intervenir au cours de l'enquête : elles sont dorénavant menées par le procureur de la République[305], et placées sous le contrôle du juge des libertés et de la détention. Elles sont prévues pour une durée initiale d'un mois, renouvelable encore une fois dans les mêmes conditions de forme et de durée.

Or, si la notion de correspondance visait principalement les lettres postales, l'émergence des nouvelles technologies de l'information et du numérique a non permis non seulement d'étendre le champ d'application de la notion aux correspondances téléphoniques, mais encore à l'ensemble des correspondances émises par la voie de communication électroniques[306], incluant de fait les SMS ou messageries instantanées comme les courriers électroniques.

Plus encore, la généralisation des réseaux sociaux de type « *Facebook* » a posé de nouvelles questions concernant le principe de vie privée, au regard notamment du fil de discussion encore appelé « *Mur* » : les paramétrages du compte d'utilisateur du réseau social détermineront ici s'il est question d'une correspondance privée, protégée par le secret, ou d'une communication au public en ligne qui lorsqu'elle

---

[302] L'article 706-73 du code de procédure pénale fixe la liste des infractions susceptibles d'entrer dans le champ de la criminalité organisée.
[303] Articles 100 à 100-7 du code de procédure pénale
[304] Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
[305] Article 706-95 du code de procédure pénale.
[306] Tribunal correctionnel de Paris, 17ème Chambre, 2 novembre 2000 : « *Sont susceptibles d'être des correspondances échangées par la voie des télécommunications soumises au secret des correspondances, les messages personnels contenus dans une messagerie électronique* ».

héberge des allégations susceptibles de constituer des faits d'apologie du terrorisme, peut donner lieu au jeu des circonstances aggravantes[307].

Parallèlement, la loi LOPPSI II a progressivement permis aux autorités judiciaires d'accéder aux données stockées au sein d'un système informatique dans le cadre des prérogatives d'enquêtes permettant de recourir aux perquisitions classiques :

Intervenant dans le seul cadre d'une information portant sur un crime ou un délit relevant du champ d'application de l'article 706-73 du code de procédure pénale, le recours au procédé était subordonné aux seules nécessités de l'information judiciaire et devait faire l'objet d'une ordonnance motivée du juge d'instruction précisant l'infraction concernée, la localisation ou la description du système informatique concerné ainsi que la durée de l'opération. Lorsque tous ces critères étaient réunis, le dispositif permettait dorénavant aux enquêteurs judiciaires d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre telles qu'elles s'affichent sur un écran pour l'utilisateur d'un STAD ou telle qu'il les y introduit par saisie de caractères, sans que le consentement des intéressés ne soit logiquement requis, ce qui suggère par ailleurs l'introduction dans le lieu d'habitation de l'intéressé devant respecter les heures légales entre 21heures du soir et 6heures du matin.

§.2/ Les moyens d'investigation prometteurs, mais intrusifs

Le procédé de géolocalisation en temps réel, si elle apparaît comme un prolongement classique des techniques de surveillance et de filatures traditionnellement mises en œuvre par la police, suscite de nouvelles questions plus problématiques pour les libertés individuelles :

Il s'agit notamment de la géolocalisation par balise GSM ou téléphone portable qui, si elle se généralise avec nouvelles technologies de l'information et du numérique, permet dorénavant aux enquêteurs de suivre non seulement le parcours de l'individu suspect en temps réel, mais plus encore de retracer l'ensemble de ses déplacements. Menace d'autant plus accentuée pour les droits et libertés fondamentaux, que ce procédé ne faisait l'objet d'aucun régime juridique précis jusqu'en 2014[308] :

La géolocalisation permettait de localiser un objet numérique posé sur un véhicule ou un ordinateur portable afin de suivre les mouvements d'un ou plusieurs suspects afin de reconstituer la carte complète des déplacements de ces derniers : tandis que la technique de localisation par satellite fût considérablement développée pour les utilisateurs de les téléphones « *intelligents* », ces outils pouvaient dorénavant être géo-

[307] Voir *infra*….Partie II, Titre I, Chapitre II, Section I, Sous-section I.
[308] Rapport du Sénat concernant le Projet de loi relatif à la géolocalisation www.senat.fr/rapl13-284-2841.html.

localisés par trois satellites distincts avec une marge d'erreur de seulement dix mètres. Les données de localisation, une fois transmises par le satellite au téléphone, étaient de nouveau transmises du téléphone à l'antenne-relais, laquelle transmettait ces mêmes données aux opérateurs de télécommunication. Par la suite, une simple réquisition de l'officier de police judiciaire amenait ces opérateurs à transférer ces données sur le serveur de la police. Il s'agissait donc non seulement d'un dispositif particulièrement intrusif dans les droits et libertés de ces utilisateurs de téléphones, mais aussi d'un procédé relativement simple à mettre en œuvre pour les autorités judiciaires. Surtout jusqu'à l'année dernière, le seul texte encadrant le recours au procédé de géolocalisation résidait « *[dans la possibilité] pour le juge d'instruction [de] procéder, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité* »[309].

L'inexistence de tout texte de loi préalable à la prise de décision du juge d'instruction, laissait à ce dernier toute la discrétion imaginable pour décider de la mise en place de ce dispositif sans qu'aucune condition légale de fond ou de forme ne soit à respecter : c'est dire que la géolocalisation pouvait concerner l'enquête de flagrance ou l'information judiciaire, viser un délit puni de six mois d'emprisonnement ou un crime puni de quinze ans de réclusion. Surtout, elle pouvait s'exercer pour toute la durée jugée nécessaire par le juge d'instruction. Le flou juridique entourant ce procédé particulièrement intrusif fût notamment sanctionné par les juges de la Cour de cassation dans deux arrêts rendus en 2014, nécessitant ainsi le développement de la sécurité juridique des particuliers face aux nouveaux dispositifs policiers sur le terrain numérique[310]

Section II / Renseignement :

Le projet de loi relatif au renseignement a été adopté à l'Assemblée Nationale le 5 mai 2015, Il sera définitivement voté lors d'un vote solennel le 9 juin 2015 : si ce texte officialise certaines pratiques anciennes (*Sous-section I*), il consacre aussi nouveaux outils controversés à disposition des services de renseignement, et consacre le privilège d'une sécurité politique dans nos sociétés (Sous-*section 2*).

§.1/ L'encadrement d'anciens outils généraux nécessaires à la prévention des menaces globales :

L'article L.811-3 du projet de loi prévoit que les services spécialisés de renseignement peuvent, dans l'exercice de leurs missions, recourir à certaines techniques couvertes par le secret[311]. Les motifs justifiant la mise en œuvre de ces techniques sont cependant publiés, ils sont au nombre de sept :[312]

[309] Article 81 du code de procédure pénale.
[310] Cour de cassation, arrêts du 22 octobre 2013, « *Géolocalisation* », n°13-81/945 et 13-81/949
[311] Les techniques sont mentionnées au Titre V du projet de loi, lequel n'est pas publié.
[312] - Impératifs d'indépendance nationale, d'intégrité du territoire et de défense nationale (1°)
- Impératifs relatifs aux intérêts majeurs de la politique étrangère et de la prévention de toute forme d'ingérence étrangère (2°)

Quand l'un de ces objectifs est poursuivi, l'article L.851-6 du projet de loi prévoit l'utilisation de dispositifs permettant de localiser en temps réel un véhicule ou un objet : l'utilisation de la technique de géolocalisation devra être autorisée par décision "(…)*écrite et motivée du Premier ministre ou d'une des personnes des assemblées parlementaires(...)*[313]", ou par "*(...)décret du Conseil d'Etat, pris après avis de la CNCTS ou des services spécialisés de renseignement relevant de ministres de la Défense et de l'Intérieur, de l'économie, du budget ou des douanes*[314]". Cependant, "*(...) en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération [de prévention des atteinte aux intérêts publics...], le dispositif mentionné [de géolocalisation] peut être installé et exploité sans autorisation préalable [mais sera susceptible de faire] l'objet d'une autorisation dans les 48heures après avis de la CNCTS.".* L'impératif de préservation des intérêts publics, ou plus globalement de la souveraineté de l'Etat sur son territoire au niveau national, permet donc de prendre des mesures de police exorbitantes à l'encontre des droits des citoyens : il conduit alors à contrôler l'exercice des libertés personnelles, afin de protéger la sécurité de l'Etat.

Parallèlement, l'article L.852-1 du second chapitre prévoit que les interceptions de sécurité, qui ne concernaient que les communications téléphoniques, est étendue aux communications électroniques : si ces mesures devront classiquement intervenir pour la sauvegarde des intérêts publics de l'Etat, elles suscitent néanmoins des problématiques quant à la préservation des libertés citoyennes.

C'est que l'article dispose que "*lorsqu'une ou plusieurs personnes appartenant à l'entourage de la personne visée par l'autorisation sont susceptibles de jouer un rôle d'intermédiaire, volontaire ou pour le compte de celle-ci, ou de fournir des informations au titre de la finalité faisant l'objet de l'autorisation, celle-ci peut être accordée également pour ces personnes*" : or, une telle mesure est susceptible de porter des atteintes disproportionnées aux personnes de l'entourage du suspect, tandis que la notion d'intermédiaire reste relativement floue. Par ailleurs, si les services de renseignement jugent nécessaire de mettre sous surveillance la personne appartenant à l'entourage du suspect initial, sur la base des seuls agissements "*volontaires ou pour le compte (...)" ainsi que la [fourniture] "d'informations*", elle laisse en suspens la question de son utilité, sinon de sa conformité avec certains faits justificatifs exonératoires de responsabilité pénale.

- Intérêts économiques, industriels et scientifiques majeurs de la France (3°)
- Prévention du terrorisme (4°)
- Prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale, de la reconstitution, action tendant au maintien de groupements dissous en application de l'article L.212-1 (5°)
- Prévention de la criminalité et délinquance organisées comme de la prévention de la prolifération des armes de destruction massive (6°)

[313] Article L.821-4 du projet de loi.
[314] Article L.811-4 du projet de loi.

C'est que l'agissement de la personne de l'entourage "*pour le compte*" du suspect principal pourrait très bien être un acte commis sous la contrainte[315], en principe exonératoire de responsabilité pénale, tandis que la fourniture d'"*informations*" pourrait se heurter au principe contenu à l'article 434-1 du code pénal selon lequel "*sont exceptés [de l'obligation de prévenir les autorités judiciaires ou administratives de la survenance d'un crime dont il est encore possible de prévenir ou d limiter les effets] les parents en ligne directe et leurs conjoints, ainsi que les frères et sœurs et leurs conjoints, de l'auteur ou complice du crime (...)*". En définitive, ces nouveaux moyens offerts aux services de renseignement privilégient nettement le principe de sécurité policière politique et militaire, sur le traditionnel principe de sécurité juridique : tandis que les intérêts publics se confondent avec les "*intérêts d'Eta*t", il s'agira notamment de "*préserver l'ordre public*" à l'intérieur des frontières, quand la "*loyauté*" est érigée en première vertu du citoyen, que la "*raison d'Etat*" justifie les immixtions dans les sphères privées. (*Voir le tableau schématique des différents modèles de sécurité contemporaine en annexe II*.)

§.2/ *La consécration de nouveaux outils spécifiques justifiés par la prévention des menaces « cyber-terroristes »* :

L'article 2 du projet de loi définit les techniques spéciales de recueil du renseignement et consacre, dans un premier chapitre, l'accès administratif aux données de connexions :

Les données de connexion peuvent être recueillies immédiatement pour les « (…) *seuls besoins de la prévention du terrorisme* »[316], pour autant qu'elles concernent des « *(...) personnes préalablement identifiées comme présentant une menace terroriste*. »[317] : L'article 2 du projet de loi prévoit donc l'installation sur les réseaux des opérateurs de téléphonie et des fournisseurs d'accès à Internet de dispositifs permettant de recueillir, en temps réel, les données de connexion ou « *métadonnées* ». On appelle ce dispositif la « *boîte noire* » :

Les données susceptibles d'être récoltées sont diverses : il s'agit des « *informations ou documents traités ou conservés par [les] réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion des services de communications électroniques [ainsi] que la liste des numéros appelés et appelants, la durée et la date des*

[315] Article 122-2 du Code pénal : "*N'est pas pénalement responsable la personne qui a agi sous l'empire d'une force ou d'une contrainte à laquelle elle n'a pu résister*"
[316] Article L.851-3 du projet de loi.
[317] *Ibidem….Supra….*

communications. »[318]. Par la suite, sur la base de ces informations, mais « *pour les seuls besoins de la prévention du terrorisme […] le Premier ministre, ou l'un des personnes déléguée par lui peut, après avis de la Commission nationale de contrôle des techniques de renseignement […] mettre en place un dispositif destiné à révéler, sur la seule base de traitements automatisés d'éléments anonymes, une menace terroriste*. »[319]. Désormais, la menace terroriste sera susceptible d'être appréhendée par le biais de l'outil numérique, sur la base des données de connexion recueillies et analysées grâce à un dispositif unique : l' « *algorithme* ».

Parallèlement, l'article L.851-7 permet dorénavant, *« lors d'opérations, l'utilisation de dispositifs mobiles de proximité permettant de capter directement les données de connexion strictement nécessaires à l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur* [ou encore] *les données relatives à la localisation des équipements terminaux utilisés*» : là encore, seule la menace de survenance d'actes terroristes justifie que ces dispositifs soient utilisés pour la captation des correspondances numériques. Cependant, si la menace terroriste est avérée, l'utilisation du dispositif pourra être autorisé dans pour une durée maximale de 144heures[320] : il permettra ainsi aux services de renseignement « *(…) d'intercepter directement les correspondances émises ou reçues [entre utilisateurs suspectés de vouloir commettre des actes de terrorisme] par l'équipement terminal*. »[321]

Chapitre III :
Emergence de nouvelles problématiques

Le projet de loi suscite de nouvelles problématiques : au niveau juridique, s'il consacre la notion contrôle des activités de renseignement par le Gouvernement, il laisse cependant en suspens la question du contrôle de l'autorité administrative instituée à cet effet (***Section I***). Au niveau sociologique, s'il privilégie le contrôle de l'activité sur Internet, il suscite de nombreuses craintes quant à l'institution d'une surveillance de masse (***Section II*).**

Section I / Problématiques spécifiques au renseignement : le contrôle

Le projet de loi sur le renseignement, s'il consacre de nouveaux dispositifs de sécurité particulièrement intrusifs dans la vie privée des citoyens, officialise cependant le contrôle non seulement gouvernemental de

[318] Ancien article L.246-1 du Code de la sécurité intérieure, devenu l'article L.851-1 après l'entrée en vigueur du projet de loi sur le renseignement.
[319] Nouvel article L.851-4 du Code de la sécurité intérieure, inséré par le projet de loi sur le renseignement.
[320] Le délai de 72heures peut être renouvelé une fois, pour la même durée.
[321] Article 2, III° du projet de loi sur le renseignement.

l'activité des services de renseignement (*Sous-section I*), mais privilégie aussi un droit de regard de l'autorité administrative indépendante, sinon de la juridiction administrative suprême (*Sous-section II*).

§.1/ Contrôle gouvernemental : le contreseing du Premier ministre

Le projet de loi prévoit différentes sortes de contrôles, parmi lesquels intervient notamment un contrôle interne :

Ce contrôle s'oriente vers deux directions, et concerne non seulement celui interne exécutif que met en œuvre le Gouvernement afin de s'assurer du bon fonctionnement et de l'efficacité des services placés sous son autorité, mais aussi un contrôle interne administratif que devra exercer tout chef de service afin de maîtriser le fonctionnement de son administration, d'impulser des réformes, de vérifier la bonne marche de la structure ainsi que la régularité des pratiques mises en œuvre comme le rappelle le rapport de l'Assemblée Nationale sur le projet de loi relatif au renseignement.

A cet égard, le contrôle du Gouvernement via le contreseing du Premier ministre présente une avancée majeure : car si les activités de renseignement étaient exercées "*dans l'ombre*" jusqu'alors, l'institution de ce type de contrôle implique la responsabilité du Gouvernement qui devra répondre des agissements commis par ces services spécialisés. Comme le relève Bertrand Warusfel, « (…) *si le projet de loi est adopté, il officialise un contrôle hiérarchique et gouvernemental sur le renseignement (...), la loi oblige le Premier ministre à contresigner (...), elle consacre la responsabilité gouvernementale* »[322].

§.2/ Contrôle administratif : le contrôle de l'autorité administrative.

La nouvelle autorité administrative indépendante instituée par le projet de loi relatif au renseignement, (la CNCTR) sera en charge du contrôle de légalité et de proportionnalité de la mise en œuvre des nouvelles techniques de renseignement. Elle sera notamment épaulée par la juridiction suprême de l'ordre administratif dans l'exercice cette tâche :

L'autorité administrative devra exercer deux types de contrôle qu'ils interviennent en aval de la procédure d'autorisation de mise en œuvre d'une technique de recueil de renseignement, ou en amont via la procédure de recours direct ou par voie préjudicielle devant le Conseil d'Etat : le contrôle de l'autorité administrative interviendra donc *a priori,* notamment par le biais de l'autorisation de mise en œuvre émanant de l'autorité administrative indépendance, ou *a posteriori* lorsqu'il s'agira d'apprécier la proportionnalité notamment du dispositif déployé pour le Conseil d'Etat.

[322] Conférence « *Mozilla Paris* », 9 avril 2015.

L'institution de ce double contrôle formel et matériel garantit théoriquement un équilibre réfléchi entre impératif de défense et de promotion des intérêts nationaux, à cheval entre principe de sécurité policière, et respect du droit au respect de la vie privée et familiale comme composante de la liberté personnelle, relevant donc de la sécurité juridique personnelle. Il s'agit donc aujourd'hui de concilier sécurité et liberté sur le plan juridique, contrôle de l'activité de l'Internet et protection des données personnelles sur le terrain numérique : cependant, seul l'exercice d'une régulation, non seulement du trafic Internet, mais encore de l'activité des pouvoirs publics pourra illustrer l'efficacité d'une telle conciliation dans l'avenir.

Section II/ Problématique liée à l'usage d'Internet : la surveillance généralisée.

L'activité de l'Internet constitue moins un outil contrôle, qu'un dispositif de contrôle des populations : à cet égard, il fait surtout craindre l'émergence d'une surveillance généralisée (*Sous-section I*).

§.1/ La présomption de culpabilité ou la surveillance généralisée

Le projet de loi sur le renseignement a suscité de vives réactions au sein de la société civile : à cet égard, ce ne sont pas moins de 28 collectifs[323], associations[324] et syndicats[325] qui se sont mobilisés contre ce texte.

Pour l'ensemble de ces acteurs, ce sont principalement les dispositifs de « *boîtes noires* » et l' « *algorithme* » qui présentent un caractère potentiellement attentatoire pour les droits et les libertés fondamentaux des internautes. Par ailleurs, la procédure de vote accélérée dont ce projet a fait l'objet suscite elle aussi des réactions, en « *l'absence de réel débat démocratique dans ce domaine […]*» selon la porte-parole du Syndicat de la Magistrature[326] (*Voir l'entretien réalisé avec M.Bonelli Laurent à cet égard en annexe I*.)

Concernant notamment le dispositif de « *Boîte noire* » fonctionnant grâce à un algorithme, le Président de Fédération « *French Data Network* » (FFDN), cofondateur de la « *Quadrature du Net* »[327], a exprimé l'étendue des risques qu'un tel dispositif engendre pour la protection des données personnelles dans une conférence organisée par « *Mozilla Paris* », en avril 2015[328] :

La « *Boîte noire* », terme générique employé pour décrire les mesures dorénavant à disposition des services de renseignement, désignerait principalement en informatique un «[*…] équipement mis en cœur du réseau*

[323] L'organisation « *Acces* », le collectif « *Café Vie Privée* » ….
[324] La Quadrature du Net, l'Association française des victimes de terrorisme, La Ligue des Droits de l'Homme, Amnesty International, Reporters Sans Frontières…
[325] Syndicat de la Magistrature, Syndicat National des Journalistes, Syndicat National des Avocats de France…
[326] Mme. BUISSON Laurence.
[327] M. BAYART Benjamin.
[328] Conférence « *Mozilla Paris* », 9 avril 2015.

qui analyserait les contenus qui y circulent[…] », quand l' « *algorithme* » viserait *« […]l' analyse en profondeur de l'ensemble des contenus afin d'en extraire une information de très haut niveau (la consultation d'un site à un instant T par une personne précise par exemple), sur laquelle on peut faire des regroupements sémantiques, qui permet finalement de déterminer les mesures qui devront être prises*». Or, la question de la détermination des mesures à prendre après analyse présenterait un réel danger ; car si l'algorithme intervient sur une population ciblée, « […] *ce ciblage reste quant à lui secret* ». De façon plus pragmatique, si « *cinq personnes anonymes sont écoutées, et que trois personnes sont suspectées, l'anonymat des trois personnes suspectées est levée, mais les cinq personnes du départ auront tout de même été écoutées*».

Ce principe de « *présomption de culpabilité* » conduirait donc les services de renseignement, pour déterminer si la loi est applicable, à violer préalablement la loi : concernant par exemple « […] *le secret des dossiers médicaux, le dispositif impliquerait qu'on aille tellement loin dans la recherche de l'information pour déterminer s'il s'agit d'un dossier médical ou non, qu'à la fin de cette recherche on ait pris connaissance de l'ensemble des informations confidentielles nous permettant de dire qu'il est bien question de ce type de dossier, théoriquement confidentiel, donc protégé»* comme le relève justement Benjamin Bayard.

En définitive, il n'y aurait confidentialité que lorsque les informations recueillies ne seraient pas utilisées à des fins d'identification de la personne concernée, tandis que l'ensemble des données circulant sur les réseaux seraient collectées, puis analysées afin de déterminer si les personnes auxquelles elles appartiennent peuvent rester anonymes ou non : il s'agirait donc plus de protéger la confidentialité de l'identité numérique des internautes, que de protéger à proprement parler la confidentialité des données personnelles.

Enfin, si l'identité numérique constitue bel et bien un droit protégé aujourd'hui[329], elle suppose nécessairement l'existence de données préexistantes (compte Internet, mots de passes, identifiants, adresse personnelle) : ainsi, l'abandon du principe de confidentialité de ces données conduirait à déterminer d'une manière relativement simple l'identité numérique d'une personne non-suspecte, protégée théoriquement par l'anonymat : la protection de la vie privée concernerait donc partiellement la réalité, mais ne saurait être préservée sur Internet.

[329] Voir *infra*…. Partie I, Titre II, Chapitre I, Section III, Sous-section II

TITRE III / Intervention de la sécurité numérique dans les interactions classiques :

Le développement de la sécurité numérique, s'il intervient notamment sein des relations interindividuelles (**Chapitre I**), questionne cependant sur l'avenir du lien d'intimité liant la population à l'Etat : il appelle à une « *autonomisation* » de la sécurité juridique, à une mise en perspective du fondement à la base du contrat social entre le citoyen et l'Etat (**Chapitre II**).

Chapitre I :
Relations interindividuelles

Le développement de la sécurité numérique entre particuliers prend de nouvelles formes quelque peu atypiques (**Section I**), quand il ne privilégie pas le retour à une « *sagesse prudente* » classique, mais nécessaire à la préservation du principe de sécurité juridique (**Section II**).

Section I / Les rencontres atypiques autour de la sécurité : les conférences « *Black Hat Europe* »

Le "*Black Hat*" revêt deux significations : il s'agit déjà d'une société fondée en 1997 par Jeff Moss, réputée pour organiser un réseau de conférences fournissant des points de vue nouveaux et exclusifs sur la sécurité de l'information, comme d'un terme employé pour désigner un hacker mal intentionné dans le monde informatique. Cependant, les deux termes convergent dans un seul sens lorsque l'on évoque les rencontres, ou conférences "*Black Hat*" : à savoir, le thème de la sécurité sur le terrain numérique.

Ces conférences rassemblent les experts des agences gouvernementales, des industries avec les hackers les plus respectés du monde : elles portent sur des thèmes techniques de la sécurité informatique et marquent un nouveau type de collaboration en matière sécuritaire. En effet, ces conférences peuvent donner lieu à l'intervention dans une même salle d'anciens patrons de la "*Central Intelligence Agency*" (CIA)[330], avant que la parole ne soit laissée à certains pirates informatiques des plus renommés, comme le collectif « *Anonymous* ».

Outre le caractère atypique de ces conférences, le niveau d'expertise qui s'y manifeste conduit à évoquer des thèmes non seulement d'une grande complexité, mais presque providentiels : à cet égard, lorsqu'en 2011, la rencontre "*Black Hat*" évoquait les possibilités offertes pour un pirate mal intentionnée de retrouver des informations personnelles sur une personne à partir de sa photo, en recourant à des technologies de reconnaissance du visage, celles de 2012 et de 2014 portaient respectivement sur les liaisons dangereuses entre le public et le privé dans le cyber-espionnage, et sur la vulnérabilité des cartes à puces pour l'avenir.

Elles illustrent alors les problématiques les plus actuelles sur le terrain numérique, et justifient une collaboration entre autorités publiques et « *pirates* » informatiques qui donne toute son efficacité à l'exercice d'une sécurité au service de l'Etat, mais aussi respectueuse des droits et libertés fondamentaux sur le terrain numérique.

Section II / Les entreprises sécuritaires alternatives

Si le Gouvernement dispose aujourd'hui d'une capacité limitée à contrôler les infractions liées au numérique, les victimes potentielles doivent plus que jamais adopter des comportements prudents (*Sous-section I*), quand la collectivité réfléchit à la création de nouveaux instruments autonomes de sécurité : à ce titre, c'est la sécurité juridique qui doit être préservée, quand celle collective doit aujourd'hui être développée (*Sous-section II*).

§.1/ Un nécessaire retour à la "sagesse prudente" :

"*De la même façon que la première chose à faire pour se prémunir des cambriolages consiste à s'assurer de ce que ses portes et fenêtre sont bien fermées, il est [aujourd'hui] quelques principes de base à respecter en matière de sécurité de l'information*"[331] :

Comme le rappellent les auteurs Peter Grabosku, Russel G.Smith et Paul Wright, l'exercice d'une simple prudence doit suffire dans de nombreux cas à préserver la sécurité *a piori* : dans cette optique, le secteur de la sécurité informatique connaît l'une des plus fortes croissances dans le monde de l'industrie et propose aujourd'hui de nouveaux dispositifs de sécurité allant de la sécurité biométrique aux programmes de détection des anomalies. Plus spécialement, un marché émerge progressivement autour des fournisseurs de services spécialisés dans des contenus adaptés à la consommation des familles. Cette sécurité peut aussi être assurée *a posteriori*, après qu'un délit ait été commis : les victimes disposent alors de recours habituels en cas de non-respect de la propriété intellectuelle[332], ou encore d'une action en dommages près les tribunaux en cas de diffamation. Par ailleurs, le nombre de recours ouverts ne concerne plus seulement à préserver les relations entre individus sur Internet, mais aussi à instituer un rapport visant à préserver les droits et libertés fondamentaux des particuliers au sein du rapport entre citoyens et autorités publiques.

Plus généralement, le développement des nouvelles technologies du numérique et des menaces susceptibles d'intervenir sur le terrain de l'Internet appelle globalement à exercer un minimum d'autorégulation, qu'elle

---

[331] "GRABOSKY Peter, G.SMITH Russel, WRIGHT Paul, "*Nouvelle technologies, nouveaux défis : crime and telecommunications*","T*rends and Issues in Crime and Criminal Justice",* 1996, n°59,

[332] Voir *infra*... Partie I, Titre II, Chapitre II, Section II, Sous-section II.

concerne d'ailleurs les fournisseurs de service ou les utilisateurs. Pour ce qui est des premiers, l'émergence comme condition d'accès d'un engagement garantissant que l'utilisateur s'interdira toute activité illégale, conduisant cas échéant à une rupture du contrat liant le particulier au fournisseur constitue déjà un instrument de protection des droits des tiers sur Internet, comme de contrôle de l'activité l'intéressant. Pour les seconds, il reste aujourd'hui libre de tout à chacun de décider du niveau de protection de la vie privée qu'il est décidé à garantir, sans oublier que tout citoyen peut constituer une victime potentielle.

Le progrès a dés lors de paradoxal son renvoi aux pratiques les plus anciennes, à la notion de sécurité la plus classique : avant de prétendre à l'exercice d'un droit à la sécurité exigible, car constituant la première garantie de nos libertés, il incombe à chacun d'assurer son propre devoir de sécurité personnelle, de préférer l'abandon d'une part de confort technologique, afin d'assumer la charge d'une responsabilité personnelle de protéger.

§.2/ Le développement autonome d'une co-production citoyenne en matière de sécurité

La coproduction citoyenne en matière de sécurité concerne les relations entre particuliers sur Internet, mais aussi les pratiques plus atypiques "*portant atteinte à la liberté de l'information, d'expression et à la neutralité du réseau*" : cette dernière mission est alors moins aux mains des autorités publiques, qu'entre celles de collectifs citoyens, dont le plus célèbre reste les "*Anonymous*"[333].

Concernant la sécurité entre particuliers sur le terrain de l'Internet, de nouvelles organisations impliquées dans des logiques de surveillance émergent progressivement sur le modèle des "*neighbourhood watch*" (surveillance de voisinage) qui désignait à l'origine un "*(...) ensemble de personnes d'un quartier, d'une rue qui s'associent dans le but de prévenir la délinquance et les cambriolages*[334]". Or, le développement des technologies du numérique a permis de transposer ces logiques sur le terrain de l'Internet : il s'agit notamment des organisations "*Simon Wiesenthal*", avec la "*Hotline CyberWtach*" ou les "*Guardian Angels*" avec notamment les "*Cyber Angels*". La "*Hotline CyberWatch*" a pour but alors de permettre à chaque internaute de dénoncer tout matériel antisémite ou raciste, quand les "*Cyber Angels*" constituent un ensemble de volontaires à la recherche de matériels illégaux concernant notamment la pornographie enfantine, le développement de virus informatiques et tout ce qui a trait au terrorisme.

Concernant le collectif "*Anonymous*" cette fois, c'est en faisant suite aux attentats intervenus au siège du journal satirique Charlie Hebdo à Paris au début de l'année 2015 que le collectif s'érige en gardien de la liberté d'expression et décide dorénavant de combattre les "*djihadistes*" sur le terrain de l'Internet : le groupe

[333] BARDEAU Frédéric, DANET Nicolas, "*Don't worry, we're from the Internet*", Dossier "*Cybermenaces : mythe ou réalité ?*", revue "*Sécurité et Stratégie"*, décembre 2012-fèvrier 2013, n°11, p.15 et ss.
[334] Définition du "*Neighbourhood watch*", Wikipedia.

d'activistes met d'ailleurs encore aujourd'hui en garde les organisations islamistes contre des représailles sur leur compte présent dans les réseaux sociaux, sous le nom de code "*@OpCharlieHebdo*[335]". Cependant, il est à rappeler qu'avant de constituer ce héraut actuel de la liberté d'expression, le collectif "*Anonymous*" restait l'ennemi de principales organisations internationales comme l'OTAN, de certaines agences gouvernementales célèbres comme le FBI ou la CIA, d'autorités nationales comme HADOPI. Plus encore, le collectif menaçait des sociétés de sécurité monnayant la protection des données, ou encore les organisations ou syndicats de défense des industries culturelles ou les multinationales protégeant leurs entreprises sur les ressources naturelles ou leurs droits de propriété intellectuelle.

Dès lors, tout ce qui porte atteinte à la liberté de l'information, d'expression et la neutralité du réseau constituait alors un "*ennemi d'Anonymous*" sans considération de structure, de taille, d'internationalisation ou de localisation sans que les opérations revendiquées par la communauté de personnes n'ait apporté d'enrichissement personnel avéré, n'ait entraîné de blessés ou de dommages irréparables.

L'émergence de ce nouveau type d'acteur démontre alors que la protection d'un objectif peut suffire à exercer n'importe quel contrôle, portant sur n'importe quelle personne quand le contrôle conduirait plus à protéger certains objectifs considérés comme primordiaux, que certaines personnes jugées plus respectables, ou considérés comme plus puissantes que d'autres : la logique du collectif "*Anonymous*" conduit alors à pleinement préserver la sécurité juridique, plutôt qu'à privilégier l'exercice d'une sécurité policière politique gouvernée par certaines affinités, à privilégier un critère purement objectif, sur des critères conjoncturels plus subjectifs.

Chapitre II

Relation Tiers – Etat :

Le rapport d'intimité liant la population et l'Etat est substantiellement affecté : il s'agit moins pour l'autorité publique de préserver les données, que de les conserver pour asseoir une surveillance basée sur le principe de présomption de culpabilité : à cet égard, la base du contrat social repose aujourd'hui plus sur l'opportunité de surveiller, que sur la responsabilité de protéger (*Section I*).

[335] L'évolution de cette opération, ayant déjà permis de pirater environ 200 comptes terroristes, peut être suivie notamment sur le site Twitter à l'adresse : https/twitter.com/hashtag/opcharliehebdo

Section I / Les fichiers de traitement des données personnelles spécifiques intéressant la sûreté de l'Etat, la défense ou la sécurité publique :

Bien que la loi "I*nformatique et Libertés*" ait prévu la possibilité pour un requérant d'obtenir la communication des informations figurant dans les fichiers « *spécifiques* » de traitement qui le concerne (*Sous-section I*), le projet de loi sur le renseignement exclue dorénavant cette possibilité (*Sous-section II*).

§.1/ Le régime juridique classique applicable aux fichiers de traitement des données personnelles spécifiques, la loi "Informatique et Libertés" :

L'article 41 de la loi "*Informatique et Libertés*" fixe le régime juridique relatif au droit des personnes à l'égard des traitements de données à caractère personnel, intéressant particulièrement la sûreté de l'Etat :

Les personnes disposent en théorie de droits de rectification, de mises à jour ou encore d'opposition à l'égard des STAD dont ils font l'objet. Surtout, ils disposent pour exercer leurs différents droits, d'un droit d'accès aux fichiers pour peu qu'ils justifient de leur identité, impliquant par la suite que les responsables de traitements communiquent les données à caractère personnel à leurs titulaires. Cependant, certains fichiers "*spécifiques*", car relatifs à la sûreté de l'Etat, la défense ou la sécurité publique, limitent l'étendue de ce droit d'accès : dans ce dernier cas, "*la demande est adressée à la CNIL qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations (qui…,lorsqu'elle la CNIL constate que) la communication des données (…) contenues ne met pas en causes les finalités (évoquées...) peuvent être communiquées au requérant*".

C'est dire que toute personne dispose d'un droit d'accès direct exigible à l'encontre du gestionnaire, ou responsable des traitements, que ceux-ci intéressent ou non la sûreté de l'Etat : la logique conduit alors à privilégier la souveraineté de l'individu, notamment de ses droits fondamentaux, sur celle de l'Etat et de ses intérêts.

§.2/ Le nouveau régime applicable aux fichiers de traitement des données personnelles spécifiques, le projet de loi sur le renseignement de 2015 :

L'article 11 du projet de loi ajoute à l'article 41 de la loi "*Informatique et Libertés*" : il conduit surtout "*(…) à préserver la confidentialité des informations (…) intéressant la sûreté de l'Eta*t" en excluant désormais tout droit d'accès direct pour l'intéressé :

L'article précité consacre deux hypothèses : selon que le traitement ou partie de traitement "*spécifique*" contienne des informations ou non sur l'intéressé. Dans le premier cas, si le traitement comporte des informations "*sensibles*", car intéressant la sûreté de l'Etat, sur une personne physique, le "(…)*Conseil d'Etat (saisi par la CNIL d'une demande d'accès formulée par la personne concernant des informations l'intéressant) se fonde sur des éléments contenus (...) dans le traitement sans les révéler, ni préciser si le requérant figure ou non dans le traitement*". Dans le second cas, lorsque le traitement ou partie de traitement comporte des données personnelles le concernant qui sont "i*nexactes, incomplètes, équivoques ou périmées, (...) dont la collecte, l'utilisation, la communication ou la conservation interdite, elle peut en informer le requérant*". Il résulte donc des deux dernières hypothèses en matière d'accès aux informations, que la personne physique ne disposera plus d'un droit réel d'accès aux informations le concernant : c'est qu'elle pourra seulement être "*informée*" de l'existence ou non d'informations la concernant, ce qui laisse un large choix discrétionnaire aux autorités publiques concernant la récolte, le traitement des données personnelles dont seul le Conseil d'Etat sera chargé d'assurer la régulation.

Dès lors, le nouvel article contenu dans le projet de loi conduit à inverser la logique relative à la conciliation entre sécurité policière et sécurité juridique, entre contrôle et protection : l'opportunité de surveiller est privilégiée sur la responsabilité de protéger, quand la "*sûreté de l'Etat*" prévaut sur la protection de la vie privée. L'outil numérique constitue moins un instrument permettant d'asseoir la souveraineté de l'individu, que d'affirmer le principe de souveraineté de l'Etat sur l'ensemble des citoyens.

Conclusion

Pour conclure, le débat sur le thème de la sécurité a toujours constitué un enjeu pour les sociétés, mais s'affranchit de ses limites traditionnelles :

C'est que les technologies du numérique viennent abolir toutes les frontières classiques, et impliquent des menaces dans notre quotidien. La sécurité, objet du débat politique dans la sphère publique, s'immisce progressivement dans la sphère privée et ne peut plus fédérer un nombre restreint de citoyens : elle nous concerne tous, lorsqu'elle imprègne les domaines les plus liés à l'intimité, notamment grâce aux nouveaux « *objets interconnectés* ».

Par ailleurs, elle vise aujourd'hui moins à préserver classiquement l'ordre public aux mains des autorités publiques, qu'à devenir un bien collectif aux mains de nouveaux acteurs. Elle revêt non seulement un caractère objectif, mais renvoie aussi au sentiment nécessairement subjectif : à cet égard, elle implique le retour à une « *sagesse prudente* », comme elle appelle à l'exercice d'une régulation réfléchie. Elle suscite notamment de nouvelles problématiques liées aux atteintes informationnelles qui, bien que s'exerçant dans la virtualité, ont des incidences dans la réalité : elle questionne la société sur le choix qu'il convient de privilégier lorsqu'il s'agit de concilier l'exercice de la liberté d'expression et préservation d'une sécurité policière, presque politique lorsqu'elle concerne le phénomène terroriste, dans une société démocratique.

Les problématiques concernant l'ajustement entre protection des droits et libertés fondamentaux numériques et contrôle de l'activité de l'Internet témoignent surtout de l'avènement d'une autre sécurité reposant sur le caractère perturbateur de la volonté humaine, nécessitant un processus d'autorégulation du système. Le principe de sécurité face aux menaces numériques viserait à garantir l'intégrité du système en prévenant toute interférence humaine, potentiellement faillible, quand le droit à la sécurité permettrait principalement d'asseoir la souveraineté du système, en excluant toute déviance personnelle. Cependant, si cette sécurité contemporaine permet de faire des « *objets interconnectés* » des nouveaux sujets, elle menace de transformer les sujets classiques (citoyens) en objets contemporains.

Pour l'avenir, le défi semble être alors de préserver la dimension humaine dans l'exercice d'une régulation adéquate, entre protection des droits et libertés numériques et contrôle de l'activité de l'Internet : il s'agirait dès lors moins de réglementer, que d'assurer le développement humain, de surveiller plutôt que de protéger. Le système reposerait moins sur la normalité que sur la responsabilité de protéger, quand la sécurité viserait plus à privilégier la souveraineté de l'individu, que la souveraineté de l'Etat.

Pour demain, le défi du droit à la sécurité consiste alors moins à être de nature policière, que d'essence humaine sur le terrain numérique.

ANNEXE I

Entretien

M. Bonelli Laurent, du 07 mai 2015

Maître de conférences à l'Université Paris-Ouest Nanterre,

Corédacteur en chef de la revue « *Culture & Conflits* »

***Question 1* :"Quand est apparu l'impératif de sécurité au cœur du débat politique français ?"**

L.B : La question de la sécurité, c'est une thématique qui émerge largement dans le débat politique français à la fin des années 1970 et qui tend à se formaliser davantage à la fin des années 1990. On a un certain nombre d'hommes politiques qui commencent à se saisir de la question de sécurité comme Alain Peyrefitte, mais elle reste réservée à de professionnels. Cependant, elle va commencer à se constituer assez largement avec des polarisations relativement importantes : à l'époque les formations de droites se définissent comme garantes de la sécurité, alors même que le parti socialiste est plus attentif aux questions de libertés publiques. Une vingtaine d'années plus tard, c'est-à-dire dans les années 90, on a un inversement de camps au colloque de Villepinte de 1997 ou se matérialise de façon particulièrement claire l'impératif politique, puisque le Premier ministre fait de la sécurité, l'une des première libertés. Cependant, il n'en fait pas exactement un droit, au sens juridique : il ne parle pas de droit à la sécurité, mais énonce plutôt la sécurité comme première des libertés, avec un basculement d'ailleurs. En effet, à ce moment "l*a gauche de gouvernement*" faisait de la délinquance la conséquence des inégalités économiques et puis finalement, on va faire de la délinquance et de l'insécurité l'une des principales causes des inégalités entre citoyens : on passe d'une conséquence des inégalités sociales, à une cause des inégalités entre citoyens. Nouvelle approche sur laquelle vont se développer tout un nombre de discours sur le "*droit à la sécurité*", mais sécurité entendue plutôt dans le sens politique, qu'à proprement parler dans le sens juridique...

***Question 2* : "D'ailleurs, la loi de 2001 sur la sécurité intérieure ajoute à l'article premier de la loi du 21 janvier 1995 proclamant le « droit fondamental à la sécurité », que ce droit est l'une des conditions de l'exercice des libertés et de la réduction des inégalités ». Selon vous, la banalisation de l'expression « sécurité » traduit-elle réellement les préoccupations de la population françaises ou relève-t-elle d'une conjoncture favorable à son emploi, notamment pour certains partis politiques ?"**

L.B : Il faut être très méfiant sur les envies de la population française, ça n'existe pas. C'est ce que pensait Bourdieu quand il disait « *l'opinion publique n'existe pas* ». Il existe cependant des groupes sociaux pour lesquels la question de la sécurité est très importante : la question de la sécurité est très liée aux relations

concrètes que ces groupes entretiennent avec d'autres groupes sociaux. Finalement, le thème de la sécurité, ou l'insécurité, est suffisamment flou pour que les gens se retrouvent sur des thèmes très différents, c'est très intéressant d'ailleurs quand on observe ce qui se passe au niveau local, ou en fait personne n'est d'accord sur les mêmes problèmes… Si on demande aux gens de faire une hiérarchie des problèmes locaux, finalement on obtient des problèmes très différents. Certains vont voir dans la prostitution, ou le phénomène des sans-domiciles-fixes un problème parce que ce sont des commerçants, qui pensent que l'image du centre-ville se dégrade, que le tourisme en souffre ; alors qu'une association qui travaille sur le quartier périphérique sera plus préoccupée par des rodéos automobiles qui vont perturber la tranquillité du quartier, etc. Parmi tous ces problèmes, ce sont les groupes qui se mobilisent et qui illustrent ce qui est dérangeant au niveau local : par exemple, pourquoi s'intéresse-t-on autant à la question des sans-domicile-fixes ? Parce qu'à la fin des années 80, premiers arrêts anti-mendicité et les premières associations se mobilisent sur ces questions. On a donc des mobilisations assez hétérogènes qui vont peser sur les élus locaux. Et ces problématiques vont trouver un écho important à la fin des années 90, avec la fin montée de l'abstention et la montée du "*Front National*" qui fait explicitement campagne sur ces thèmes de la sécurité. Les élus se mettent dans une position de reconquête de ces questions de sécurité, et font campagne sur ce thème. La sécurité va constituer un des enjeux, sans qu'il y ait nécessairement un lien entre ce que disent les élus à l'Assemblée Nationale et ce qui se passe dans leur circonscriptionla réalité. On peut dire la sécurité est le problème de tous, mais si on dit tous la même chose on ne peut plus faire deu débat politique, il faut donc trouver des écarts distinctifs…

<u>Question 3</u> : "Depuis 1995, et à deux reprises par la suite (loi de 2001 et de 2003), le législateur parle d' « un droit fondamental à la sécurité » : ces dispositions seront reprises dans le Code de la sécurité intérieure de 2012. Vingt ans après, au regard notamment de ces événements de ce début d'année, existe-il réellement un « droit fondamental à la sécurité ? »

L.B : l'Etat s'est construit sur le "*monopole de la violence légitime*". Mais la violence physique légitime, ce n'est pas quelque chose qui à avoir avec les citoyens, mais plutôt avec la sécurité de l'Etat. Ainsi, l'Etat s'assure qu'il a le monopole de la force armée, et qu'aucun autre groupement ne peut contester les armes à la main sa légitimité : c'est ça la question de la sécurité. Cette question s'étend d'ailleurs au privé, comme continuation de cette logique. C'est l'Etat qui gère la justice, avec l'idée qu'on ne peut pas faire justice soi-même, avec l'auto-défense qui est punie sévèrement car appartenant au monopole de l'Etat. Au fond, les problèmes de la petite délinquance ont souvent été aux mains d'autres acteurs sociaux que l'Etat : c'était les industriels locaux qui géraient l'ordre social dans les usines par exemple, mais à l'extérieur des usines également...Or, depuis une quarantaine d'années, on a une sorte de fonctionnalisation de la question de l'ordre, comme si toutes ces questions appartenaient à l'Etat : c'est lui qui a à gérer la délinquance., mais c'est un phénomène très nouveau. Sous ce nouveau rapport, on est donc dans une logique où l'Etat aurait

l'obligation de garantir la sécurité, alors que l'ordre social fonctionnait car il reposait sur un modèle disciplinaire décritfondé notamment depuis par Michel Foucault. La question de l'ordre est à la fois quelque chose de très récent finalement, sans nécessairement que ça ait tant de réalité que ça...

<u>Question 4</u> : "L'influence de plus en plus marquée des organisation terroristes, véhiculée notamment par le biais des nouveaux médias comme les réseaux sociaux (on parle de "cyberdjihaddistes") ou Youtube (le documentaire "Flame of Wars" notamment) marque une nouvelle étape dans le processus de radicalisation des jeunes occidentaux. A ce titre, la loi du 13 novembre 2014 relative à la lutte contre le terrorisme a été votée par le législateur : s'agit-il selon vous d'un outil nécessaire et adapté aujourd'hui ?"

L.B : Tout d'abord je relativiserai l'idée selon laquelle il y a plus de terroristes aujourd'hui qu'auparavant : en réalité si vous prenait la fin du XIXème siècle on a un phénomène de terrorisme bien plus marqué et présent avec la violence ethno-nationaliste qui a causé ainsi bien plus de morts que celle djihadiste dans les pays occidentaux. Par ailleurs, aussi dramatiques qu'ils soient, les attentats de janvier 2015 ont pu toucher des victimes nombreuses certes, mais ceux de 1995 ont causé un traumatisme bien supérieur : les attentats ont eu lieu dans le métro, on causé plus de blessés, et illustrent une violence bien plus marquée que les attentats de janvier : en 1995, c'est presque l'état de siège. Les menaces terroristes ne sont donc pas vraiment nouvelles, d'autant que ce qui se passe en Irak et en Syrie traduit la volonté de l'Etat islamique qui est d'asseoir son autorité sur ces territoires : en levant l'impôt, en assurant la justice… Dans cette lutte, ils utilisent la propagande qui peut avoir un certain effet d'attraction sur un nombre de jeunes européens : là encore, il faut faire attention. Il y avait avant des jeunes partant pour la guerre d'Espagne, les volontaires français contre le bolchevisme, les suisses contre le Nicaragua ; il y 'a aujourd'hui des jeunes qui vont se battre en Ukraine, donc on a toujours des flux très importants de gens qui vont se battre sur d'autres fronts, ce qui n'implique pas que tous les gens qui reviennent par la suite constituent une menace réelle pour leur pays d'origine. Le risque existe, il y a certes une grosse probabilité que cette menace survienneque certains passent à l'acte : pour autant, il n'y a aucun caractère mécanique à cela. Ce ne sont pas des choses qui se confondent complétement. Ce que font Kouachi et Coulibaly, ça renvoie à des trajectoires très singulières : passer à l'attentat ce n'est pas exactement la même chose que d'aller au s'engager dans un conflit lointain. Je pense que la propagande ne fonctionne que chez des gens prédisposés à ce qu'elle marche chez eux : je ne crois pas sociologiquement que parce qu'on voit un message, on passe à l'action. Peut-être qu'un clip de l'Etat islamique peut jouer, mais ça signifie que le spectateur est déjà dans une situation telle qu'il est réceptif à ce message. La propagande a moins un rôle concret sur desdonne un sens aux actions des individus, mais n'en est que très rarement le moteur. que sur des individus prédisposés à passer à l'action : et l'action, ils y passeront qu'il y ait ou pas Internet.

<u>Question 5</u> : "La loi sur le renseignement a été prise pour des motifs de sécurité intérieure : elle suscite des controverses, notamment à l'égard des utilisateurs d'Internet qui craignent une surveillance de masse. Que pensez-vous de ce texte ?"

L.B : Je pense que le problème se trouve dans le caractère potentiellement subversif de cette loi: il y'a unle déséquilibre flagrant entre les motifs invoqués pour la loi, et les raisons pour lesquelles elle a été prise, ce qui est problématiquepose question du point de vue du débat démocratique. On peut avoir un vrai débat sur la surveillance, et sur ses limites mais prendre un texte sous le prétexte d'une utilisation officielle (l'antiterrorisme), alors qu'il s'agit d'une toute autre utilisation (l'espionnage), ça pose un vrai problème. Il s'agit en effet d'un texte opaque, qui utilise des termes techniques : en l'occurrence, c'est une loi qui sous l'angle de la surveillance de métadonnées met en place des outils dont les contreparties en matière de libertés sont importantestrès faibles. On a eu le débat avec les pratiques de la NSA, or cette agence avait le souci d'éviter les citoyens américains : en France, on n'est pas discriminant, et on traite les Français comme des étrangers en l'alignant sur le bas, en ne protégeant personne. Peut-être que l'utilisation de ce dispositif sera contrôlé, cependant dès lors que le dispositif est mis en place, on peut s'interroger sur l'équilibre entre nécessité et liberté... D'autant que la France reste un pays doté d'un système anti-terroriste puissant, et intrusif dans les libertés publiques si nécessaire... Je pense qu'il n'y a pas eu la sérénité et la profondeur nécessaire pour prendre la loi qui sera sans doute la plus intrusive de la cinquième République.

SECURITE JURIDIQUE	SECURITE COLLECTIVE	SECURITE POLICIERE (POLICE GENERALE)	SECURITE POLICIERE (POLICE POLITIQUE)	SECURITE POLICIERE (POLICE TOTALIT AIRE)	SECURITE MILITAIRE (CLASSIQUE)	SECURITE MILITAIRE (CONTEMPORAIN)	SECURITE HUMAINE*
Contrat social	Pacte des Nations	Conservation des biens et des personnes	Préservation de l'ordre public	Poursuite du mouvement	Système *West-Phalien*	Guerre froide	Souffrance des populations
Liberté	Droit des peuples à disposer d'eux-mêmes	Réglementation	Etat d'exception	Mobilisation	*Jus ad bellum*	Bipolarité Dissuasion	Développement humain
Propriété	Intégrité territoriale	Surveillance	Maintien de l'ordre Renseignement	Participation à la Cause Vérification	Intérêts d'Etat	Sphère d'influence	Protection des populations
Egalité	Egalité souveraine	Normalité	Loyauté	Conformisme	Raison d'Etat	Alignement idéologique	Responsabilité de protéger
Solidarité	Mécanismes de secours et d'entraide	Délation	Dénonciation	Signalement et aveu	Balance des puissances	Equilibre des menaces principe d' indiscutable	Souveraineté de l'individu

ANNEXE II

Tableau synthétique des différents concepts de sécurité contemporaine

(« *Le Principe Sécurité »,* Frédéric Gros, Gallimard Essais, 2012, Appendices)

*Le principe de « *sécurité humaine* », bien que développé par le philosophe Frédéric Gros, ne figure pas dans le tableau synthétique développé dans son ouvrage. L'ajout de ce principe résulte d'une initiative personnelle, propre à illustrer la cohérence de ce travail de mémoire.

INDEX

TABLE DES MATIERES

- SECONDE PARTIE –

BIBLIOGRAPHIE

Ouvrages :

§. Philosophie classique :

- *« Leviathan ou Traité de la matière, forme et du pouvoir d'une république ecclésiastique et civile », Thomas Hobbes, 1651*
- *« Le Traité du gouvernement civil », John Locke, Londres, 1690.*
- *« De l'esprit des lois », Montesquieu, Genève, 1748*
- *« La nouvelle Héloïse », Jean Jacques Rousseau, 1761, Paru chez Marc Michel Ray*
- *« Le Contrat Social », Jean Jacques Rousseau, 1762, Paru chez Marc Michel Rey*

§. Philosophie contemporaine :

- *« Surveiller et punir », Michel Foucault, Editions Gallimard Essais, 1975*
- *« Histoire de la folie à l'âge classique », Michel Foucault, Editions Gallimard, 1972.*
- *« Post-scriptum sur les sociétés de contrôle », Gilles Deleuze, l'Autre Journal, 1990*
- *« Le Principe Sécurité » Frédéric Gros, Editions Gallimard Essais, 2012.*
- *« Social Networking as a Stage of Grammatization and the New Political Question », Bertrand Stiegler, 2013.*

§. Sociologie :

- *« Le Savant et le Politique », Max Weber, Paris, Union Générale des Editions, 1919*
- *« La Société du Risque : sur l'autre voie de la modernité », Ulrich Beck, Edition Champs Essais, 2008*
- *« La France a peur, Une histoire sociale de l'insécurité », Laurent Bonelli, Editions La Découverte, 2010*

§. Général :

- *« Le Neuromancien », William Gibson, Editions Ace Books, 1984*
- *« Cybernetics », Norbert Wiener, Paris Hermann, 1984*
- *« Histoire du XXème siècle : la fin du monde européen », Tome 1, Serge Bernstein et Pierre Milza, Editions Hatier, 1996.*
- *« Histoire du XXème siècle : le monde entre guerre et paix », Tome 2, Serge Bernstein et Pierre Milza, Editions Hatier 1996.*

- *« La sécurité humaine : un concept pertinent ? » Mary Kaldor, Institut Français des Relations Internationales, Politique Etrangère, 2006, 350 pp.*
- *« 100 dates de la Culture générale », Eric Cobast, Collection « Que Sais-Je ? », Editions PUF, 2009*
- *« The Fouth Paradgim : Data scientific intensive discovery », Tony Hey, Stewart Tansleu, Tolle Kristin, Microsoft Research, 2009, 284 p.*
- *« Histoire du XXème siècle : la fin du monde bipolaire », Tome 3, Serge Bernstein et Pierre Milza, Editions Hatier, 2010*
- *« 100 mots de la Culture générale », Eric Cobast, Collection « Que Sais-Je ? », Editions PUF, 2010*
- *« La cyber-sécurité », Nicolas Arpagian, Collection « Que Sais-Je ? », Editions PUF, 2010*
- *« Le renseignement criminel », François Farcy, Jean François Gayraud, Editions Biblis, 2014*
- *« Big Data, penser l'homme et le monde autrement », Gilles Babinet, Editions Le Passeur, 2015*
- *« Le piège « Daech », l'Etat islamique ou le retour de l'histoire », Jean Pierre Luizard, La Découverte, 2015.*

Manuels :

- *« Droits et libertés fondamentaux », Louis Favoreu, Précis Dalloz, 4eme Edition, 2007*
- *« Cyber droit : le droit à l'épreuve de l'Internet », Christiane Féral-Schuhl, Dalloz, 6ème Edition, 2010*
- *« Le guide des infractions », Jean-Christophe Crocq, Dalloz, 16ème Edition, 2014*
- *« Le droit de la sécurité intérieure », Emmanuel Dupic, Editions Gualino, 2014.*
- *« Informatique, Télécoms, Internet », Alain Bensoussan, Editions Francis Lefebvre, 2012.*
- *« Manager les données publiques : ouverture, exploitation, valorisation », Kober Vincent, Edition Territorial, 2014.*
- *« Manuel de droit européen en matière de protection des données », Agence des droits fondamentaux de l'Union Européenne, Conseil de l'Europe, 2014.*
- *« Objets connectés : sécurité juridique et technique », Piette-Coudol Thierry, Editions LexisNexis, 2015.*

Articles, Chroniques, Commentaires :

- *« Nouvelles technologies, nouveaux défis », Peter Grabosky, Russel G. Smith, Paul Wright, « Trends and Issues in Crime and Criminal Justice », n°19, 1996*
- *« Tiers de confiance ou de défiance ? La sécurité collective face à la cryptographie asymétrique », Gaël Boisseau, Cahiers de la sécurité intérieure, Institut National des Hautes Etudes sur la Sécurité et la Justice, n°34, 4° trimestre 1998*
- *« Detecting influenza epidemics using search engine query data », J. Ginsberg, Revue Nature, Volume 457, 19 fèvrier 2009.*

- *« Network Neutrality, Boradland Discrimination », Tim Wu, Journal of Telecommunications and High Technology Law, Vol.2, 2003.*
- *« Les menaces numériques aujourd'hui », « Dossier - 2010-2020 : une nouvelle décennie de menaces ? », Philippe Wolf, Revue « Sécurité et Stratégie » n°3, 2010.*
- *« Enquête EDHEC-CDSE : Panorama 2008 et 2009 des crimes commis contre les entreprises », « Dossier - 2010-2020 : une nouvelle décennie de menaces ? », Philippe Very, Bertrand Monnet, Olivier Hassid, revue « Sécurité et Stratégie », n°3, mars 2010.*
- *« Le défi des nouveaux usages numériques : la sécurité des entreprises à la peine », « Dossier - Cybermenaces : mythes ou réalités ? », Bruno Gruselle, Revue « Sécurité et Stratégie » n°11, décembre 2012-fèvrier2013*
- *« Nouvelles technologies et crime désorganisé : incursion au cœur d'un réseau de pirates informatiques », « Dossier - Cybermenaces : mythes ou réalités ? », Benoit Dupont, Revue « Sécurité et Stratégie » n°11, décembre 2012-fèvrier2013*
- *« Quelle place pour l'option « cyber » dans notre sécurité nationale ? », Compte rendu du rapport de M.Jean-Marie Bockel au nom de la Commission des Affaires Etrangères et de la Défense et des Forces Armées du Sénat, juillet 2012, Nicolas Arpagian. Revue « Sécurité et Stratégie », n°11, 2012.*
- *« Don't worry, we're from the Internet », Dossier – « Cybermenaces : mythes ou réalités ? », Frédéric Bardeau, Nicolas Danet, revue « Sécurité et Stratégie », n°11, décembre 2012-fèvrier2013*

Rapports, Projets :

- *Rapport « Tricot », TRICOT Bertrand, 1975*
- *Livre Blanc de la « Défense et Sécurité Nationale », « La Documentation Française », juin 2008.*
- *Rapport du Conseil d'Etat, « Les autorités administratives indépendantes », La documentation Française, 2001*
- *Rapport de la Commission sur la sécurité humaine, SEN et OGATA, du 16 octobre 2003*
- *Rapport du Sénat sur le « Projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers », n°117, 6 décembre 2005.*
- *Note technique du Ministère de l'intérieur, de l'outre-mer et des collectivités locales, « la vidéo-protection intelligente », juillet 2008.*
- Rapport de l'UNESCO, « *Freedom of connection – freedom of expression* », William Dunton, Anna Dopatka, Ginette Law, Victoria Nash, Unesco Series on Internet Freedom, 2011.
- *Rapport de l'Inspection Générale des Finances, « Soutien à l'économie numérique et à l'innovation », 25 octobre 2012; www.economie.gouv.fr/soutien-a-economie-numérique-et-a-innovation-publication-rapport-igf.*
- *Rapport d'information, Commission des lois constitutionnelles de la législation et de l'administration générale de la République, MM. Jean Jacques Urvoas et Patrice Verchère, 14 mai 2013*

- *Rapport du Conseil d'Etat, « Le numérique et les droits fondamentaux », La documentation Française, 2014*
- *Rapport du Sénat relatif au « Projet de loi sur la géolocalisation », n°374, 18 février 2014,*
- *Rapport du Sénat sur le « Projet de loi relatif au renseignement », 19 mars 2015.*

Droit national :

§. Textes à valeur constitutionnelle :

- *Déclaration des Droits de l'Homme et du Citoyen de 1789*
- *Constitution du 4 octobre 1958*
- *Préambule du 27 octobre 1946*

§. Codes :

- *Code pénal, version consolidée du 28 mars 2015.*
- *Code de procédure pénale, version consolidée du 1 mai 2015.*
- *Code de la sécurité intérieure, version consolidée du 18 mai 2015*
- *Code de la propriété intellectuelle, version consolidée du 11 mai 2015.*
- *Code de justice administrative, version consolidée du 18 avril 2015.*
- *Code général des collectivités territoriales, version consolidée du 9 mai 2015.*
- *Code de commerce, version consolidée du 29 mai 2015.*

§. Lois :

- *Loi du 29 juillet1881 sur la liberté de la presse.*
- *Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*
- *Loi n°85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle.*
- *Loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.*
- *Loi n°88-13 du 5 janvier 1988 d'amélioration et de la décentralisation.*
- *Loi du 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.*
- *Loi n°95-73 du 21 janvier 1995d'orientation et de programmation relative à la sécurité.*
- *Loi n°96-659 du 26 juillet 1996 de réglementation des télécommunications.*

- *Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.*
- *Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.*
- *Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.*
- *Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*
- *Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.*
- *Loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité.*
- *Loi n°2014-344 du 17 mars 2014 relative à la consommation.*
- *Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.*

Jurisprudence

§. Juge administratif :

- *Ordonnance, Conseil d'Etat, « Commune de Mandelieu La Napoule », 20 juillet 2001*
- *Ordonnance, Conseil d'Etat, « Deperthes » 9 janvier 2001*
- *Ordonnance, Conseil d'Etat, « Hébergement d'urgence », 10 février 2012.*

§. Juge judiciaire :

- *Jugement, Tribunal correction de Paris, 17° chambre, 2 novembre 2000.*
- *Arrêt, Cour de cassation, Chambre criminelle, 22 octobre 2013.*

§. Juge constitutionnel :

- *Décision n°71-44 DC du 16 juillet 1971, « Loi relative à la liberté d'association »*
- *Décision n°80-127 DC du 20 janvier 1981 "Loi Sécurité et Liberté".*
- *Décision n°81-132 DC du 16 janvier 1982, « Loi relative aux nationalisations »*
- *Décision n°99-505 DC du 18 juin 1999 "Loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs."*
- *Décision n°2009-580 DC du 10 juin 2009, « Loi favorisant la diffusion et la protection de la création sur Internet. »*

Droit européen et communautaire :

§. Conventions

- *« Convention Européenne des Droits de l'Homme », 4 novembre 1950.n°184*
- *« Charte des droits fondamentaux de l'Union Européenne », 7 décembre 2000.*
- *« Convention pour la Protection des personnes à l'égard du traitement automatisé des données personnelles », 28 janvier 1981, n°108*
- *« Convention sur la Cybercriminalité », 23 novembre 2001, n°185.*

§. Jurisprudence

- *CEDH, « Kruslin c/ France », 24 avril 1990, n°11801/85.*
- *CEDH, « Marper c/ Royaume-Uni », 4 décembre 2008, n°30562/04 et n°30566/04*
- *CJUE, « Digital Rights Ireland Seitlinger e.a », 8 avril 2014, n°94/2014.*
- *CJUE, « Google Spain », 13 mai 2014, n°C/131-12.*

§. Directives

- *« Directive services de médias audiovisuels », Parlement européen et Conseil de l'Europe, 10 mars 2010, n°2010/13/UE.*
- *« Directive relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur », Parlement européen et Conseil de l'Europe, 8 juin 2000, n°2000/31/CE*
- *« Directive relative au traitement des données à caractère personnel et relative à la protection de la vie privée dans le secteur des communications électroniques », Parlement européen et Conseil de l'Europe, 12 juillet 2002, n°2002/58/CE.*
- *« Directive relative au service universel et aux droits des utilisateurs au regard des réseaux et services de communication électronique », Parlement européen et Conseil de l'Europe, 25 novembre 2009, n°2009/136/CE.*

§. Décisions

- *« Décision relative à la signature au nom de l'Union Européenne et les Etats Unis d'Amérique sur le traitement et le transfert des dossiers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure », Conseil de l'Europe, 23 juillet 2007, n°2007/551/PESC/JAI*

Droit International :

- *Déclaration Universelle des Droits de l'Homme, 10 décembre 1948*
- *Pacte International relatif aux Droits Civils et Politiques, 16 décembre 1966*
- *Pacte International relatif aux Droits Economiques, Sociaux et Culturels, 16 décembre 1966*

Discours officiels :

- *Déclaration officielle, Lionel Jospin, Colloque de Villepinte, 19 juin 1997*
- *Déclaration officielle, Jacques Chirac, Salon international de l'alimentation, octobre 2000.*
- *Discours sur l'état de l'Union, George Bush, 29 janvier 2002.*
- *Compte rendu intégral des débats du Sénat, Robert Badinter, séance du 20 janvier 2004.*
- *Déclaration du ministre de l'Intérieur, Bernard Cazeneuve, 4 février 2015.*

Journaux, Quotidiens, Sites :

- *« Deux concepts de la souveraineté », Kofi Annan, « Le Monde », 22 septembre 1999.*
- *« Le Parlement européen donne son feu vert à l'accord PNR avec les Etats-Unis », Actualité, Parlement européen, 19 avril 2012*
- *« Les cinq chiffres (fous) de la vidéosurveillance », Camille Polloni, « Les Inrocks », juin 2012.*
- *« Déclaration de Vinton Cerf : nous devons défendre la liberté sur Internet », 4 décembre 2013, www.lemonde.fr*
- *« Ecoute et espionnage : les Français sous surveillance », George Moras, 15 décembre 2013, www.lemonde.fr*
- *« Plan vigipirate : comment un dispositif exceptionnel est devenu permanent », Leila Marchand, 24 avril 2014, www.lemonde.fr*
- *"Objets connectés, humains chômeurs : de l'utopie numérique au choc social", Evgeny Morozov, "Le Monde Diplomatique", Août 2014.*
- *« Géopolitique de l'espionnage », Dan Schiller, « Le Monde Diplomatique », Novembre 2014.*
- *"Les données personnelles au cœur d'une bataille juridique : privés de vie privée", Jerôme Thorel, "Le Monde Diplomatique", janvier 2015.*
- *« Loi sur le renseignement en France : feu vert sur la surveillance de masse », Félix Tréguer, « Le Monde Diplomatique », juin 2015.*
- *« Les nouveaux moyens de lutte contre un terrorisme en « libre accès » et protéiforme », Ministère de l'Intérieur, Mars-Avril 2015, « Civique Magazine », n°226.*
- *"7 jours face au terrorisme", Ministère de l'Intérieur, Janvier-Février 2015, "Civique Magazine", n°225.*

- *« Le difficile retour en France des « repentis » du départ en Syrie », Julie Hamaïde, 5 avril 2015, slate.fr.*
- *« Le Parlement européen négocie son engagement sur le PNR européen », Euractiv.com, l'Europe dans le monde, News, 25 février 2015.*

Vidéothèque :

§. Cinéma

- *« L'Aveu », réalisation : Costa Gavras, Drame-Thriller, 23 avril 1970*
- *« Minority Report », réalisation : Steven Pielberg, Science-Fiction, 2 octobre 2002*
- *« Transcendance », réalisation : Wally Pfister, Science-Fiction, 25 juin 2014*
- *« A Most Violent Year », réalisation J.C Chandor, Drame,16 Novembre 2014*

§. Documentaires

- *« Citoyens sous surveillance : un œil sur vous », réalisation : Valentin Alexandre , 25 mars 2015, Arte TV*
- *« Une contre histoire de l'Internet », réalisation : Bergere Sylvain, 15 mai 2013, Arte TV*
- *« Djihad 2.0 », réalisation : Toscer Oliver, 1 mai 2015, LCP Assemblée Nationale*

Divers :

- *Conférence « Mozilla Paris », BLISSON Laurence (Syndicat de la Magistrature), BAYART Benjamin (Représentant de la FFDN, Quadrature du Net), RIHAN CYPEL Eduardo(député PS de la 8ème circonscription de la Seine et Marne), MARTIN Daniel (Président de l'Institut International des Hautes Etudes de la Cybercriminalité), WARUSFEL Bertrand (Docteur d'Etat en Droit), 9 avril 2015.*